IBM SmartCloud Entry

Administrator Guide 3.1

IBM SmartCloud Entry

Administrator Guide 3.1

Note

Before using this information and the product it supports, read the information in "Notices" on page 171.

Fourth Edition (June 2013)

Contents

Chapter 1. IBM SmartCloud Entry Administrator Guide 1

Chapter 2. What's new in IBM SmartCloud Entry 3

Chapter 3. Key concepts 5

Chapter 4. Planning for IBM SmartCloud Entry 7

Recommended hardware 7
Supported software versions 7
IBM SmartCloud Entry server components . . . 8
IBM SmartCloud Entry client components . . . 9
Prerequisite software components 9
Scalability and performance considerations 12
Server and concurrent user maximums 12
Cloud management system metrics tuning (VMControl) 13

Chapter 5. Installing prerequisite software 15

IBM Systems Director VMControl prerequisite installation 15
Downloading and installing IBM Systems Director and VMControl 15
Applying prerequisite fixes for IBM Systems Director 6.3.x and VMControl 2.4.x 16
Applying prerequisite fixes for IBM Systems Director 6.2.x and VMControl 2.3.x 17
Configuration considerations for IBM Systems Director and VMControl 18
VMware prerequisite installation 21
Microsoft Hyper-V prerequisite installation 21
Database prerequisites (optional) 22
Downloading and installing DB2 22
Creating a DB2 database for IBM SmartCloud Entry 22

Chapter 6. Installing IBM SmartCloud Entry 23

New installation on Windows 23
Graphical installation (default) 23
Console installation. 24
Silent installation 25
New installation on Linux or AIX 26
Console installation (default) 26
Graphical installation 28
Silent installation 29
Applying fixes and updates for IBM SmartCloud Entry 30
IBM SmartCloud Entry for Cloud SSL configuration (optional) 31
Connecting using SSH 33

Chapter 7. Migrating IBM SmartCloud Entry 35

Migrating to a new release 35
Migrating your configuration 35
Migrating your data 36
Migrating configuration manually 36
Migrating from one system to another 37
Migrating from version 2.4 to a version 3.1 appliance 37
Migrating a Derby database to DB2 database . . . 38

Chapter 8. Starting and stopping IBM SmartCloud Entry 41

Chapter 9. Uninstalling IBM SmartCloud Entry 43

Uninstalling a graphical installation of IBM SmartCloud Entry on Windows. 43
Uninstalling a console installation of IBM SmartCloud Entry on Windows. 43
Uninstalling IBM SmartCloud Entry on Linux or AIX 44
Uninstalling a graphical installation of IBM SmartCloud Entry on Linux or AIX 44
Database cleanup 45

Chapter 10. Deploying IBM SmartCloud Entry Virtual Appliances for System x . 47

Prerequisites for IBM SmartCloud Entry Virtual Appliances 47
Deploying the Hyper-V virtual appliance 47
Deploying the KVM virtual appliance 52
Deploying the VMware virtual appliance 53
Managing the IBM SmartCloud Entry appliance . . 56
Enabling OpenStack services on KVM and VMware 56
Generating authentication tokens 57
Managing passwords 57
Starting, stopping, and status of the IBM SmartCloud Entry application on IBM SmartCloud Entry for System x virtual appliance . 58
Volume group management for the IBM SmartCloud Entry appliance. 58
Performing support and maintenance tasks on the IBM SmartCloud Entry for System x appliance 61

Chapter 11. Installing the IBM SmartCloud Entry Hyper-V Agent . . . 63

IBM SmartCloud Entry Hyper-V Agent Installation Prerequisites 63

Installing on Microsoft Windows Server 2012 or Microsoft Hyper-V Server 2012 64
Creating installation or uninstallation logs . . . 64
Installing with graphical Installation 65
Installing with silent installation 67
Changing encrypted passwords after installation 70
Uninstalling the IBM SmartCloud Entry Hyper-V Agent 71
Uninstalling the IBM SmartCloud Entry Hyper-V Agent on Microsoft Hyper-V Server 2012 71
Enabling nova migration CLI from Hyper-V . . . 72
Enabling Microsoft Hyper-V Server 2012 systems for ISO generation 73
Starting and stopping services 73
Supporting an additional vSwitch on the Hyper-V compute node 73

Chapter 12. Configuring IBM SmartCloud Entry home directory properties 77

Configuring user registry authentication. 78
LDAP authentication 78
Configuring LDAP authentication manually . . 78
Changing authentication mode 80
Configuring local authentication 80
Configuring REST API authentication. 81
Configuring database 82
Configuring email notifications 83
Configuring common cloud properties 83
Cloud refresh interval 83
Cloud online help configuration 84
Configuring global image deployment 84
Configuring a deployment target 85
Configuring cloud synchronization mode . . . 86
Configuring a staging project 86
Configuring global priority of an instance when relocating 87
Configuring access to advanced deployment form 87
Configuring the number and maximum size of additional storage 88
Configuring Storage Copy Services (SCS) capture repositories (VMControl only) 88
Configuring retry for a failed deploy or delete action (VMControl only) 89
Configuring images with VMware. 89
Configuring images with OpenStack 96
Configuring instance resize timeout 103
Identifying expired instances 103
Virtual appliance label translations 104
Configuring multiple instances for a single deployment 104
Configuring logging 105
Configuring a network 105
Configuring billing 107
Configuring billing 107
Configuring billing details 108
Configuring metering. 110
Configuring web user interface 111
Configuring user interface widgets 111
Configuring session timeout 112
Configuring the Welcome page 113
Configuring the default instance name 113

Chapter 13. Configuring IBM SmartCloud Entry from the web interface 115

Configuring the default administrator user account 115
Configuring LDAP authentication using the web interface 115
Images 116
Building images 116
Importing images (OpenStack only) 117
Updating an image configuration strategy (OpenStack only) 118
Creating a VMware linked virtual machine . . 118
Configuring image deployment properties. . . 119
Deploying an image 121
Copying image definitions 122
Viewing image properties 123
Deleting images 123
Projects 123
Project membership roles 123
Creating a project 124
Editing project properties 124
Managing projects. 125
Deleting an existing project. 126
Project management with OpenStack 127
Approval policies 127
Setting or modifying approval policies for a cloud 127
Setting or modifying approval policies for a project. 128
Requests 129
Processing instance requests 129
Clearing or archiving requests. 130
Expiration policies. 130
Updating the default expiration policy for a cloud 131
Updating the default expiration policy for a project. 131
Flavors (OpenStack only) 131
Updating the flavor for an OpenStack cloud configuration 131
Multiple cloud support 132
Adding a cloud configuration 132
Configuring an OpenStack cloud 132
OpenStack clouds 133
Removing a cloud. 134
Updating a cloud 134
Network configurations 134
Managing network configurations 135
Adding a network configuration 135
Editing network configurations 138
Managing IP address pools. 138
Instances 140
Capturing an instance 141
Pinning an instance 141
Processing requests from the Instances tab. . . 141
Hiding or showing an instance 141
Resizing an instance (VMControl) 142

Resizing an instance (VMware) 142
Resizing an instance (OpenStack). 143
Users 143
Creating a user 144
Viewing or updating a user 144
Unlocking a user 144
Deleting a user 144
User management with OpenStack 144
Accounts 145
Creating an account 145
Add members to an account 146
Viewing or managing an account. 146
Deleting an account 146
Clearing or archiving events 146

Chapter 14. Security 147

Chapter 15. Best practices for using IBM SmartCloud Entry 149
Back up and restore IBM SmartCloud Entry . . . 149
Using the **screen** command 150
Using the **nohup** command 150
Deploying 500 virtual servers to a VMControl cloud in a 24 hour period 151

Chapter 16. IBM SmartCloud Entry for System X 153
IBM Systems Director Standard Edition 153
Tivoli Provisioning Manager for Images 153

Chapter 17. Troubleshooting 155
IBM SmartCloud Entry FAQ 155
Logging tasks 156
Change logging levels from the OSGi command prompt 156
Retrieve log and system files 157
Troubleshooting using the OSGi console 158
Known issues 159
Two users within the same browser 159
Display issue with Internet Explorer. 159
No billing information for processor and memory products 160
Duplicate FCPorts causes IBM Systems Director to lose its zoning information for the VIOS servers 161
IBM SmartCloud Entry shows instance in 'Stopped' state even though the deployment was successful 161
Delete and add instance failures under load . . 162
Instance in Error state cannot be deleted . . . 162
Delete of an instance while a storage flashcopy is running against the instance will cause the delete to fail. 163
IBM Systems Director unexpectedly stops logging 163
Failures noticed during server relocation or editing of virtual server properties 163
PKI error when adding OpenStack cloud . . . 164
Error opening sockets to server when using DB2 164
Limitations 165
Starting IBM SmartCloud Entry on a high scale cloud 165
Limitations when using VMware within the IBM SmartCloud Entry 165
DNS and domain name restrictions for VMControl AIX deployments 166
Include only ASCII characters in configuration files 166
Maximum REST API connection limit in VMControl 166
Disk resize support 166
Target restrictions for VMControl IBM i deployment 166
Use of network configurations provided by Network Control is not supported 167
The install path cannot contain non-English characters 167
Limitation on specifying a large memory or number of processors. 167
Limitations when you deploy an image . . . 167
Direct usage of OpenStack CLI or REST APIs prohibited 168
Unable to restore a virtual server with fixed VHD type 168
Validation errors when updating a configuration strategy 168

Accessibility. 169

Notices 171
Trademarks 172
Privacy policy considerations 173

Chapter 1. IBM SmartCloud Entry Administrator Guide

With IBM SmartCloud® Entry, you can maintain control over the allocation of resources with a web-based application.

IBM SmartCloud Entry is implemented as a lightweight web-based application that runs as an Open Services Gateway initiative (OSGi) application.

You can perform common public or private cloud operations such as:
- Providing access to multiple clouds from a single portal
- Provisioning and de-provisioning servers
- Drafting and cloning instances
- Capturing instances
- Starting and stopping servers as part of an instance
- Resizing existing virtual machines
- Creating projects to give team-specific access to instances
- Providing network configurations, which set unique network properties to different instances
- Creating expiration polices to reduce abandoned virtual machines
- Providing request and approval workflow support
- Monitoring resource allocations and billing for services

IBM SmartCloud Entry uses the following FIPS 14-2 approved cryptograhic providers:
- IBMJCEFIPS (certificate 376)
- IBMJSSEFIPS (certificate 409)
- IBM® Crypto for C (certificate 384)

The certificates are listed on the NIST website at http://csrc.nist.gov/cryptval/140-1/1401val2004.htm.

For more information about the IBM SmartCloud Entry capabilities that are available for the User role, see the IBM SmartCloud Entry User Guide.

Chapter 2. What's new in IBM SmartCloud Entry

Learn about new features in the IBM SmartCloud Entry 3.1 release.

The new features include the following:

- Support for the Microsoft Hyper-V hypervisor using OpenStack technologies. OpenStack is an open source cloud-computing platform for public and private clouds.

  IBM SmartCloud Entry supports the following features with Microsoft Hyper-V:
  - Image management
  - Windows and Linux images
  - Flavor management
  - Secure shell (SSH) key management
  - Deploy and resize disk
  - Backup and restore
  - IPv4 / IPv6 network management
  - Projects, approvals, expirations, billing and metering
- OpenStack is now integrated and pre-configured into the IBM SmartCloud Entryappliances for VMware, KVM and Hyper-V.
- Ability to suspend and resume an instance on all cloud types.
- Ability to create multiple configurations of a virtual image. Additionally, the virtual image can exist in more than one project.
- Support for secure access to LDAP servers. LDAP authentication provides the highest level of security for production environments.
- Ability to set user Secure Shell (SSH) keys during deployment to VMware, vCenter, and Hyper-V environments.
- Support for images that are generated with the IBM Image Construction and Composition Tool and allow secure access through public and private key pairs.
- Ability to resize a disk during deployment is now available for the VMControl cloud type.
- Ability to attach storage using N_Port ID Virtualization (NPIV) when you are deploying to a system pool when you are using a VMControl cloud type in a Power Systems™ environment.
- Ability to enable remote restart to maintain availability of your virtual servers and workloads within a server system pool, when you are using a VMControl cloud type.
- Enhancements added for the VMware cloud type:
  - Support for customizing user data when you are deploying an image. For more information, see "Setting VMware user data during deployment" on page 93.
  - Support for setting a user password and SSH public key for a guest operating system during deployment. For more information, see "Set secure access during deployment" on page 94.
  - Support for a delay before powering off an instance to allow the virtual machine to complete its shutdown process. For more information, see "Configuring shutdown of VMware instances" on page 96.
  - Support for linked clones. For more information, see "Creating a VMware linked virtual machine" on page 118.
- Terminology update: What was called an *appliance* in previous versions of IBM SmartCloud Entry is now called an *image* in the web interface and documentation. What was called a *workload* in previous versions of IBM SmartCloud Entry is now called an *instance* in the web interface and documentation.

The support updates include the following:

- IBM Systems Director VMControl™ 2.4.3 support
- Safari browser on an iPad

Chapter 3. Key concepts

IBM SmartCloud Entry supports many different types of virtualization infrastructure environments. These environments use different terminology for the same concepts and are described in the following table.

Note: IBM SmartCloud Entry is aligning more closely with OpenStack terminology. For example, workload and appliance are now referred to as an instance and image. OpenStack is an open source cloud-computing platform for private and public clouds. For information about OpenStack, see http://www.openstack.org/

Table 1. A terminology comparison between the virtualization infrastructure type and the IBM SmartCloud Entry equivalent term

Virtualization infrastructure type	Term	Definition	IBM SmartCloud Entry equivalent
VMware	Template	A blueprint of a virtual machine containing the metadata and one or more disk images that can be used to create new virtual machines.	Image
VMware	Virtual machine	A runnable instance of a virtual computer, similar to a physical computer that runs an operating system and applications.	Instance
VMControl	Workload	A virtual computer, similar to a physical computer that runs an operating system and applications.	Instance
VMControl	Virtual appliance (resulting in a single virtual machine)	An image of a virtual machine that can be used to create new virtual machines.	Image
OpenStack	Flavor	A flavor is a defined size for a provisioned virtual machine. Each flavor has a unique combination of resource configurations and sizes.	Flavor

In addition to terminology differences between environments, there are key concepts that you must understand.

Projects
IBM SmartCloud Entry projects provide a management realm to group images and instances that only the members of that project can see and manage.

Requests
Requests are any actions that require administrator approval before they can complete. IBM SmartCloud Entry sends an approval request when a user attempts an operation that an IBM SmartCloud Entry administrator has set up to require approvals.

Accounts
Enabling the billing operation in IBM SmartCloud Entry activates the account feature. An account

includes a balance, an owner, an account balance threshold, account members, and invoices. The account members are charged for the instances that they deploy.

Note: Only IBM SmartCloud Entry administrators can create accounts, but an IBM SmartCloud Entry user can be assigned as an account owner.

Basic and advanced deployments

Users deploy an image by using the basic deployment form. Project owners or administrators can use the basic or the advanced deployment forms. They can also configure which deployment settings are shown on the basic deployment form.

Chapter 4. Planning for IBM SmartCloud Entry

This section provides information on planning for IBM SmartCloud Entry, including recommended hardware and software for the various IBM SmartCloud Entry components.

Recommended hardware

This section describes hardware recommended for various platforms supported by IBM SmartCloud Entry.

The information provided is a general guideline and actual requirements can vary from installation to installation. Specific sizings should be done to meet your installation requirements.

The IBM SmartCloud Entry server is supported on the following platforms:

- Intel x86-64 (Windows or Linux)
- POWER6® or POWER7® (AIX®)

This table describes both the minimum hardware requirements and recommended minimum production hardware requirements for the IBM SmartCloud Entry server component.

The minimum requirements listed indicate the absolute minimum hardware levels needed when running with only 5-10 concurrent users.

The recommended minimum production requirements are recommendations to support a small cloud. As with any software solution, hardware needs to be properly sized for a specific customer scenario.

Table 2. Minimum hardware requirements

Component	Minimum hardware requirements	Recommended minimum hardware production requirements
IBM SmartCloud Entry server [1]	0.5 CPUs 650 MB free disk space 1 GB physical memory	2 CPUs 25 GB free disk space 8 GB physical memory
IBM SmartCloud Entry appliance	2 CPU 60 GB free disk space 4 GB physical memory	(With Hyper-V and OpenStack Support) 4 CPUs 60 GB free disk space 8 GB physical memory
[1]Requirements are for the IBM SmartCloud Entry server only. If other servers, such as the Director server, are installed on the same system, the requirements would need to be higher to account for the additional needs of the other components installed and running there.		

Supported software versions

This section provides the software versions supported by IBM SmartCloud Entry.

The supported versions listed are current at the time of publication. See the IBM SmartCloud Entry wiki for any updates. Also see “Applying prerequisite fixes for IBM Systems Director 6.3.x and VMControl 2.4.x” on page 16 for the instructions on getting the latest fixes required by IBM SmartCloud Entry.

IBM SmartCloud Entry server components

The following tables list the supported components that are required by the IBM SmartCloud Entry server.

Table 3. Supported operating systems

Operating system	Versions	Notes
AIX	6.1 (64-bit) TL5 or 7.1 (64-bit)	With latest fix pack
Red Hat Enterprise Linux	Version 6.1, 6.2, and 6.3 (64-bit)	With latest fix pack
Windows Server 2008	R2 (64-bit)	With latest fix pack
Windows Server 2012 Datacenter		

Table 4. Supported databases

Database	Versions	Notes
Integrated Derby		
DB2®	9.7, and 10.1	With latest fix packs

Table 5. Supported user registries

User registry	Versions	Notes
IBM SmartCloud Entry	Local identity storage and authentication	• The IBM SmartCloud Entry database is used to store identity artifacts including credentials. • Intended for proof of concept scenarios or for performing a demo. • Intended for small scale usage; one to approximately 30 users and projects.
LDAP Version 3	IBM Tivoli® Directory Server Version 6.1	• Supported by the latest fix pack. • Intended for production environments to provide the highest level of security. • Scales to hundreds or thousands of users and projects. • TLS (transaction level security) is supported.
Active Directory	6.1.7601.17514	• Supported by the latest fix pack. • Intended for production environments to provide the highest level of security. • Scales to hundreds or thousands of users and projects. • TLS (transaction level security) is supported.

IBM SmartCloud Entry client components

The following table lists the supported component versions for clients that access the IBM SmartCloud Entry servers.

Note: Clients or versions that are not listed here might still work.

Table 6. Browser compatibility

Browser	Versions	Notes
Internet Explorer	9.0 or 10.0	With latest fix pack Minimum resolution of 1024x768 (or greater) Internet Explorer 9 or 10 compatibility view is not supported
Firefox ESR	17	With latest fix pack Minimum resolution of 1024x768 (or greater)
Chrome	23	With latest fix pack
Safari	6	With latest fix pack

Prerequisite software components

IBM SmartCloud Entry has additional software prerequisites, which vary depending on the type of cloud provider that you use.

IBM SmartCloud Entry is dependent on one of the following providers for platform management and virtualization services:

- Microsoft Hyper-V
- IBM Systems Director VMControl
- VMware vSphere with vCenter

Microsoft Hyper-V prerequisites

IBM SmartCloud Entry is compatible with the following versions of Microsoft Hyper-V products:

Table 7. Supported Microsoft Hyper-V products

Microsoft Hyper-V products	Versions
Microsoft Hyper-V Server 2012[1]	
Windows Server 2012 with Hyper-V role enabled	• Standard Edition • Datacenter edition

1. To use Microsoft Hyper-V Server 2012 with IBM SmartCloud Entry, you must install a compatible ISO generation utility such as genisoimage from Cygwin. For more information, see "Enabling Microsoft Hyper-V Server 2012 systems for ISO generation" on page 73.

IBM Systems Director VMControl prerequisites

IBM SmartCloud Entry is compatible with specific versions of IBM Systems Director and IBM Systems Director VMControl.

To use the full functionality of IBM SmartCloud Entry, the most current version of IBM Systems Director and IBM Systems Director VMControl is required.

Note: If you are running IBM Systems Director and VMControl on a PureFlex™ system, install the latest Flex Systems FSM fix packs. For more information, see the IBM Flex Systems information center topic Updating systems at http://publib.boulder.ibm.com/infocenter/flexsys/information/topic/com.ibm.director.updates.helps.doc/fqm0_t_um_updating_systems.html.

IBM SmartCloud Entry works with the following versions of IBM Systems Director and IBM Systems Director plug-ins:

Table 8. Version support for IBM Systems Director and IBM Systems Director VMControl

IBM Systems Director server	Versions	Notes
IBM Systems Director 6.3.3.x with IBM Systems Director VMControl	IBM Systems Director 6.3.3 IBM Systems Director VMControl Enterprise Edition 2.4.3	With latest fix pack
IBM Systems Director 6.3.2.x with IBM Systems Director VMControl	IBM Systems Director 6.3.2 IBM Systems Director VMControl Enterprise Edition 2.4.2	With latest fix pack
IBM Systems Director 6.3.x with IBM Systems Director VMControl	IBM Systems Director 6.3.1.1 IBM Systems Director VMControl Enterprise Edition 2.4.1.1	With latest fix pack
IBM Systems Director 6.2.x with IBM Systems Director VMControl	IBM Systems Director 6.2.1.2 IBM Systems Director VMControl Enterprise Edition 2.3.1.2 IBM Systems Director VMControl Standard Edition 2.3.1.2 (limited support[1])	With latest fix pack
IBM Systems Director Storage Control (optional) [2]	4.2.4 4.2.3 4.2.2.1 4.2.1	With latest fix pack
IBM Tivoli Storage Productivity Center (optional) [2]	4.2.1 interim fix 1	With latest fix pack[3]
IBM Systems Director Service and Support Manager (optional)	6.3.3 6.3.2 6.3.1 6.2.1	With latest fix pack
SMI Agent (optional) [4]	120.11.0	With latest fix pack

1. For more information about limited support, see Chapter 5, "Installing prerequisite software," on page 15.
2. For N_Port ID Virtualization (NPIV) support, at least one of IBM Systems Director Storage Control or IBMTivoli Storage Productivity Center products must be installed.
3. For the latest information, see the IBM Tivoli Storage Productivity Center Latest Downloads technote at https://www-304.ibm.com/support/docview.wss?uid=swg21320822.
4. If you are using IBM Systems Director Storage Control or IBMTivoli Storage Productivity Center, then you must use the SMI Agent.

IBM SmartCloud Entry uses IBM Systems Director VMControl application programming interfaces (APIs) to deploy new servers through Storage Copy Services (SCS) using the Integrated Virtualization Manager (IVM) or Hardware Management Console (HMC) and Virtual I/O Server (VIOS). The following are the supported versions for this SCS-based Power Systems virtualization environment.

Table 9. Supported versions for the Storage Copy Services Power Systems Virtualization environment

Managed servers	Versions	Notes
PowerVM®	PowerVM Enterprise Edition	
Kernel Virtual Machine (KVM)		
Virtual I/O Server (VIOS)	VIOS 2.2.2.2	With latest fixes[1] Dual VIOS is supported
Hardware Management Console (HMC)	HMC V7R7.6.0.0	With latest fixes
Integrated Virtualization Manager (IVM)	IVM 2.2.2	With latest fixes
1. The list of VIOS fixes can be viewed on the Fix Central website at http://www-933.ibm.com/support/fixcentral		

Supported configurations for storage

IBM SmartCloud Entry uses IBM Systems Director VMControl. IBM Systems Director VMControl supports provisioning based on Storage Copy Services (SCS) through IBM Systems Director Storage Control or an external IBM Tivoli Storage Productivity Center.

Supported storage and switches depend on the level of IBM Systems Director that you are using. For information about supported storage and switches, see the Supported storage devices in the IBM Systems Director information center at http://pic.dhe.ibm.com/infocenter/director/pubs/topic/com.ibm.director.plan.helps.doc/fqm0_r_hardware_compatibility_storage_devices.html.

VMware prerequisites

IBM SmartCloud Entry is compatible with the following versions of VMware products:

Table 10. Supported VMware products

VMware products	Versions	Notes
VMware vCenter Server 4	Standard edition (version 4.1 update 1) Essentials (version 4.1 update 1)	For more information, see "VMware prerequisite installation" on page 21.
VMware vCenter Server 5	Standard edition Essentials edition Editions that are listed are supported at version 5.1.0 and 5.1 update 1.	

Table 10. Supported VMware products (continued)

VMware products	Versions	Notes
VMware vSphere 4	Standard edition (version 4.1 update 1) Advanced edition (version 4.1 update 1) Enterprise edition (version 4.1 update 1) Essentials Plus (version 4.1 update 1)	
VMware vSphere 5	Standard edition Essentials Plus edition Enterprise edition Enterprise Plus edition Editions that are listed support the following versions: • 5.0.0 • 5.1 • 5.1 update 1	

Scalability and performance considerations

IBM SmartCloud Entry offers considerations with regard to scalability and performance within the cloud environment.

Server and concurrent user maximums

Depending on your cloud manager, IBM SmartCloud Entry supports a different number of users and servers in the environment.

It is assumed that the environment includes enough physical hardware to perform at these levels.

Table 11. Server and concurrent user maximums

Microsoft Hyper-V cloud manager	VMware cloud manager[1]	VMControl cloud manager[2, 3]
• 50 concurrent users of the IBM SmartCloud Entry user interface or APIs • 500 maximum virtual servers	• 50 concurrent users of the IBM SmartCloud Entry user interface or APIs • 3000 maximum virtual servers	• 50 concurrent users of the IBM SmartCloud Entry user interface or APIs • 500 maximum virtual servers on IBM Power Systems Group Rack Models that are using VIOS without implementing shared storage pools • 1000 maximum virtual servers for KVM, IBM PureFlex Power Systems, and IBM Power Systems Group Rack Models that are using shared storage pools [4, 5] • 200 virtual disks per host

Table 11. Server and concurrent user maximums (continued)

<table>
<tr><th>Microsoft Hyper-V cloud manager</th><th>VMware cloud manager[1]</th><th>VMControl cloud manager[2, 3]</th></tr>
<tr><td colspan="3">1. For more information about VMware configuration maximums, see the VMware configuration maximums (v4) PDF at http://www.vmware.com/pdf/vsphere4/r40/vsp_40_config_max.pdf and VMware configuration maximums (v5) PDF at http://www.vmware.com/pdf/vsphere5/r50/vsphere-50-configuration-maximums.pdf.
2. For more information about performance tuning and scaling, see the Performance Tuning and Scaling Guide for IBM Systems Director 6.3 at http://www.ibm.com/support/docview.wss?uid=nas7139a0e4d2c6aa65c8625797b006e6aeb.
3. For more information about best practices, see Virtualization Best Practices wiki at http://www.ibm.com/developerworks/wikis/display/virtualization/Virtualization+Best+Practice.
4. Recommend no more than 30 virtual servers (for example, LPARS) per managed system as it can affect I/O through VIOS and discovery and inventory update times.
5. A single Hardware Management Console (HMC) should not manage more than 800 virtual servers for the IBM Systems Director VMControl cloud.</td></tr>
</table>

Cloud management system metrics tuning (VMControl)

Monitoring large numbers of managed resources can negatively affect performance on the management server. Adjusting appropriate polling intervals helps to minimize the negative performance impacts. IBM Systems Director provides a configurable polling interval for virtualization monitors which determines how often requests are made for metrics data for a managed resource.

For more details on configuring HMC metrics and IBM Systems Director polling intervals, see the following resources:

HMC metrics:

Setting the HMC to collect resource utilization data for managed systems in the IBM Systems Director Information Center. at http://publib.boulder.ibm.com/infocenter/director/v6r2x/index.jsp?topic=/com.ibm.director.virtualization.helps.doc/fqm0_t_vm_enabling_hmc_metrics.html

IBM Systems Director VMControl:

Polling intervals for virtualization monitors in the IBM Systems Director Information Center at http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.status.helps.doc/fqm0_c_polling_intervals_vsm_main.html.

IBM SmartCloud Entry recommends running with a 5 minute sampling rate on HMC and a 5 minute interval on IBM Systems Director. The IBM Systems Director sampling rate is defined in the file `/opt/ibm/director/data/vsmmetric.properties`. These are the specific Director properties that can be set.

```
# Represents the frequency at which the management server polls the platform
# services.
DirectorPollingInterval=300000

# Represents the frequency at which the platform services poll a managed
# resource.
PlatformPollingInterval=300000

# Represents the frequency at which the Power Systems platform services
# poll a managed resource.
PowerPlatformPollingInterval=300000

# Represents the frequency at which the Power Systems platform services
# poll a managed resource for utilization data.
PowerPlatformUtilizationPollingInterval=300000
```

```
# Represents the frequency at which the Power Systems platform services
# poll a managed resource for allocation data.
PowerPlatformAllocationPollingInterval=300000
```

Chapter 5. Installing prerequisite software

This section lists the prerequisite software that is required for the various virtualization cloud types to run IBM SmartCloud Entry.

IBM Systems Director VMControl prerequisite installation

For the VMControl cloud type, IBM SmartCloud Entry is dependent on IBM Systems Director VMControl Enterprise Edition, which includes system pool support, to perform deployments and other virtualization operations to more than one host. System pool support allows a group of servers to be used as a cloud and also facilitates upgrade to IBM higher-end service management cloud offerings. Therefore, before you install IBM SmartCloud Entry, ensure that your VMControl server environment is completely setup and ready to create workloads from virtual appliances.

IBM SmartCloud Entry has limited support for targeting a single host as a deployment target. A single host can be specified as the deployment target for either Global virtual appliance configuration or for Individual virtual appliance configuration, but a single host cannot be set during deployment or during approval of a deployment. This use of a single host as the deployment target requires only IBM Systems Director VMControl Standard Edition support.

Setting up and configuring IBM Systems Director and IBM Systems Director VMControl is out of the scope of this document, but here is a list of useful links for downloading, installing, configuring, and troubleshooting VMControl to manage a POWER® environment:

Downloading and installing IBM Systems Director and VMControl

This topic contains links to the IBM Systems Director information center and the IBM Redbooks® website to help you download, install, and troubleshoot IBM Systems Director and IBM Systems Director VMControl.

Downloading

Download the versions of IBM Systems Director and IBM Systems Director VMControl from the IBM Systems Director download page at http://www.ibm.com/systems/software/director/downloads/index.html. IBM Systems Director is available from the Management servers page and IBM Systems Director VMControl is available from the Plug-ins page.

Installing and configuring

Find information about installing, upgrading, and migrating IBM Systems Director and IBM Systems Director VMControl from the IBM Systems Director Resource page at http://www.ibm.com/systems/software/director/resources.html.

When you are configuring the managed IBM DB2 database for IBM Systems Director, ensure that there is significant free space on the file system that contains the database so that it can create temporary objects. By default, the managed IBM DB2 database for IBM Systems Director is in `/home/dirinst1`. At least 3 GB of free space is required for IBM SmartCloud Entry to deploy images and complete other functions. If IBM Systems Director is managing 1,000 workloads, then 5 GB of free space are required for the managed IBM DB2 database.

Troubleshoot

- IBM Systems Director troubleshooting forum at http://www.ibm.com/support/search.wss?rs=0&q=eServerOnDemandKBRCH&r=100&sort=desc

- IBM Systems Director VMControl troubleshooting forum at http://www.ibm.com/support/search.wss?rs=0&lang=en&loc=en_US&r=10&cs=utf-8&rankfile=0&cc=us&coll=0&spc=&stc=&apar=include&q1=vmcontrol&q2=&sort=rk&tc=&ibm-search.x=16&ibm-search.y=9&dc=&dtm

Note: The links provided here are subject to change without notice.

Applying prerequisite fixes for IBM Systems Director 6.3.x and VMControl 2.4.x

The latest updates are required for IBM Systems Director and VMControl before you install IBM SmartCloud Entry. These updates are available for download and installation from the Fix Central download page.

About this task

Note: You should install the latest available fix pack for IBM Systems Director and VMControl before you install prerequisite fixes.

Specific software levels or fixes (for example, HMC, VIOS) might also be required on the target hosts for IBM Systems Director and VMControl to properly manage the client virtual servers. These fixes are available for download from the IBM SmartCloud Entry Fix Central page.

The current list of prerequisite software fixes is as follows:

- For IBM Systems Director fixes, use fix ID: **vmc-update.2.4.1.0-iFix:SCEentitled**

The most current information for IBM SmartCloud Entry, including the latest documentation, installation instructions, and support and fixes, can be found on the IBM SmartCloud Entry wiki at https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/W21ed5ba0f4a9_46f4_9626_24cbbb86fbb9/page/Support%20and%20Fix%20Instructions.

The IBM SmartCloud Entry wiki provides details about specific fixes available and instructions for downloading and installing them.

Download and install the prerequisite fixes as outlined in the following steps.

Procedure

1. Open your browser to IBM Support Fix Central at http://www-933.ibm.com/support/fixcentral/.
2. Select **Select product**.
3. Select **Other Software** for the Product Group.
4. Select **IBM SmartCloud Entry** for the Product.
5. Select **All** for the Installed Version.
6. Select **All** for the Platform.
7. Select **Continue**.
8. On the identify fixes page, enter the following text into the **individual fix ids** field: `vmc-update.2.4.1.0-iFix:SCEentitled`. Click **Continue**.
9. On the select fixes page, select the `vmc-update.2.4.1.0-iFix` file. Click **Continue**.
10. Authenticate as required.
11. Select the method that you want to use to download the fix and click **Continue**.
12. Click the `vmc-update_2.4.1.0_20120522-iFix.zip` file to download
13. View the `readme.html` file that is listed along with the fix pack download file.

    The readme file contains instructions for applying the prerequisite fixes. If you choose to download using your browser or HTTP, you can also view the readme file online.

14. Repeat steps 7 through 12 for any additional fix IDs provided in the current list of prerequisite software fixes.

What to do next

Before you install a fix pack or upgrade IBM SmartCloud Entry, back up your `skc.ini` file to a safe location. After you install the fix pack or finish upgrading, replace the `skc.ini` file with your backup version.

Applying prerequisite fixes for IBM Systems Director 6.2.x and VMControl 2.3.x

The latest updates are required for IBM Systems Director and VMControl before you install IBM SmartCloud Entry.

About this task

Specific software levels or fixes (for example, HMC, VIOS) might also be required on the target hosts for IBM Systems Director and VMControl to properly manage the client virtual servers.

The current list of prerequisite software fixes is as follows:

- For IBM Systems Director fixes, use fix ID: **2.2.0.0-SKC-ISDBASE_LAFIX1:SKCentitled**
- For IBM Systems Director VMControl fixes, use fix ID: **.2.0.0-SKC-VMC_LAFIX2:SKCentitled**
- For the embedded version of IBM Tivoli Storage Productivity Center fixes, use fix ID: **2.2.0.0-SKC-SC_4_2_1_a_AIX:SKCentitled**
- For HMC fixes, use fix ID: **2.2.0.0-SKC-HMC .iso:SKCentitled**

The most current information for IBM SmartCloud Entry, including the latest documentation, installation instructions, and support and fixes, can be found on the IBM SmartCloud Entry wiki at https://www.ibm.com/developerworks/mydeveloperworks/wikis/home?lang=en#/wiki/W21ed5ba0f4a9_46f4_9626_24cbbb86fbb9/page/Support%20and%20Fix%20Instructions.

The IBM SmartCloud Entry wiki provides details about specific fixes available and instructions for downloading and installing them.

Download and install the prerequisite fixes as outlined in the following steps.

Procedure

1. Open your browser to IBM Support Fix Central at http://www-933.ibm.com/support/fixcentral/.
2. Select **Select product**.
3. Select **Other Software** for the Product Group.
4. Select **IBM Starter Kit for Cloud** for the Product.
5. Select **All** for the Installed Version.
6. Select **All** for the Platform.
7. Select **Continue**.
8. On the identify fixes page, enter the following text into the **individual fix ids** field: `2.2.0.0-SKC-ISDP-IF20110831:12S8192K701C91734`. Click **Continue**.
9. On the select fixes page, select the `2.2.0.0-SKC-ISDP-IF20110831` file. Click **Continue**.
10. Select the method that you want to use to download the fix and click **Continue**.
11. View the `readme.html` file that are listed along with the fix pack download file.

    The readme file contains instructions for applying the prerequisite fixes. If you choose to download using your browser or HTTP, you can also view the readme file online.

12. Repeat steps 7 through 12 for any additional fix IDs provided in the current list of prerequisite software fixes.

What to do next

Before you install a fix pack or upgrade IBM SmartCloud Entry, back up your `skc.ini` file to a safe location. After you install the fix pack or finish upgrading, replace the `skc.ini` file with your backup version.

Storage management related fixes (VMControl 2.3.x only)

IBM Systems Director VMControl enables you to use IBM Tivoli Storage Productivity Center to manage your enterprise storage systems. In this case, IBM Systems Director VMControl uses IBM Systems Director Storage Control which uses embedded management interfaces for TPC to manage storage devices.

For more information about IBM Tivoli Storage Productivity Center and IBM Systems Director, see the Using IBM Systems Director Storage Control 4.2.1 with IBM Tivoli Storage Productivity Center in the IBM Systems Director Information Center at http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.storagectrl.helps.doc/fqm0_t_sc_using_with_tpc.html.

Alternatively, you may have an IBM Tivoli Storage Productivity Center server installed and running in your environment where IBM Systems Director discovers and uses the IBM Tivoli Storage Productivity Center server to manage your storage.

In each of these environments where IBM Tivoli Storage Productivity Center is used, there are IBM Tivoli Storage Productivity Center fixes required to do provisioning through IBM Systems Director VMControl and IBM SmartCloud Entry; therefore, IBM Tivoli Storage Productivity Center must be updated to the following fix levels:

With the full, stand-alone version of IBM Tivoli Storage Productivity Center installed and employed, the IBM Tivoli Storage Productivity Center 4.2.1 FP6 or later is required.

With the embedded version of IBM Tivoli Storage Productivity Center, the IBM Tivoli Storage Productivity Center hot fix is available along with other IBM SmartCloud Entry fixes on the IBM Support Fix Central website. For more information about downloading and installing the fix, see the IBM SmartCloud Entry wiki at https://www.ibm.com/developerworks/mydeveloperworks/wikis/home/wiki/IBM Starter Kit for Cloud/page/Support and Fix Instructions

Configuration considerations for IBM Systems Director and VMControl

Using hosts or system pools for NPIV deploying

N_Port ID Virtualization (NPIV) is an industry-standard Fibre Channel (FC) technology that allows the Virtual I/O Server to directly share a NPIV-capable FC adapter between multiple client partitions. For NPIV, the Virtual I/O Server acts as an FC pass-through instead of a SCSI emulator such as when using virtual SCSI. To enable IBM SmartCloud Entry to take advantage of this functionality provided by IBM Systems Director VMControl, follow the instructions in the IBM PowerVM Virtualization Introduction and Configuration Redbook at http://www.redbooks.ibm.com/abstracts/sg247940.html?Open. Look for requirements and information about configuring the VMControl support NPIV through Storage Copy Services (SCS) in Chapter 2.8.

Using system pools for advanced placement

For IBM SmartCloud Entry to take advantage of the advanced placement functionality that is provided by IBM Systems Director VMControl, you must complete some additional configuration steps. This advanced placement functionality is provided by VMControl server systems pools.

After this configuration is completed, you can deploy instances (workloads) from the IBM SmartCloud Entry to a VMControl server system pool. VMControl server system pools are required for the actual deployment of the workload, including intelligent workload placement to the host servers in the system pool.

When you are using IBM Systems Director VMControl with system pools, configure the systems in the pool with similar capabilities to allow for LPAR mobility across the pool, including the networks that are defined on the systems and features such as Active memory Expansion (AME).

Before putting systems into a pool, make sure that you have your environment set up.

- For more information about setting up your environment for IBM Systems Director VMControl 2.3.x, see Preparing your Power Systems environment for server system pools topic in the IBM Systems Director VMControl information center at http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.vim.helps.doc/fsd0_vim_t_preparing_environment_for_pools.html.
- For more information about setting up your environment for IBM Systems Director VMControl 2.4.x, see Preparing your Power Systems environment for server system pools topic in the IBM Systems Director VMControl information center at http://publib.boulder.ibm.com/infocenter/director/pubs/topic/com.ibm.director.vim.helps.doc/fsd0_vim_t_preparing_environment_for_pools.html.

Setting up and configuring IBM Systems Director VMControl System Pools is out of the scope of this document, but can be found in the following locations:

- For IBM Systems Director VMControl 2.3.x, see Managing server system pools topic in the IBM Systems Director VMControl information center at http://publib.boulder.ibm.com/infocenter/director/v6r2x/topic/com.ibm.director.vim.helps.doc/fsd0_vim_t_managing_pools.html.
- For IBM Systems Director VMControl 2.4.x, seeManaging server system pools topic in the IBM Systems Director VMControl information center at http://publib.boulder.ibm.com/infocenter/director/pubs/topic/com.ibm.director.vim.helps.doc/fsd0_vim_t_managing_pools.html.

Configuring remote restart capability

For IBM SmartCloud Entry to use the remote restart capability that is provided by IBM Systems Director VMControl, you must complete some additional configuration steps if you are using Power Systems hosts.

About this task

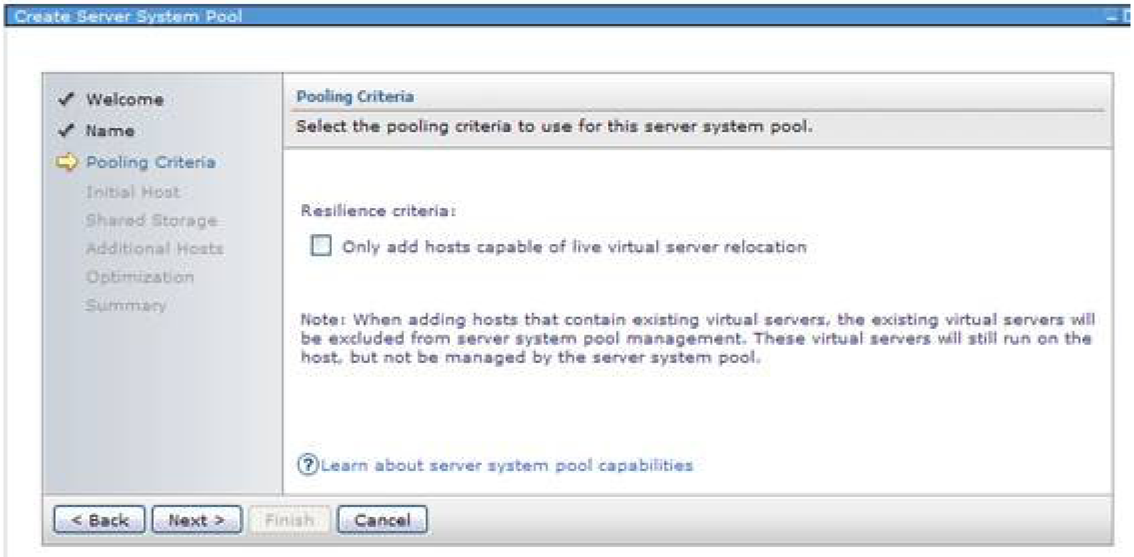
When remote restart is enabled, if a host fails, virtual servers on the host can be automatically restarted on another host in the server system pool. You can create instances (workloads) in IBM SmartCloud Entry that are enabled for remote restart. First, you must create one or more reserved storage devices that have enough available space to contain the configuration data of the deployed virtual server. You create these reserved storage devices by using the Hardware Management Console (HMC). For more information, see Creating reserved storage devices for remote restart resilience in Power Systems environments in the IBM Systems Director information center at http://pic.dhe.ibm.com/infocenter/director/pubs/topic/com.ibm.director.vim.helps.doc/fsd0_vim_t_preparing_environment_for_pools_remote_restart.html.

Mobility of servers within a system pool

When using IBM Systems Director VMControl version 2.3.1.2, the mobility of a server must be disabled within a system pool. When using IBM Systems Director VMControl version 2.4.1, you can manually enable the mobility of the server.

About this task

To disable mobility when using VMControl version 2.3.1.2, uncheck the box under Resilience criteria in the VMControl Create Server System Pool wizard as follows:



Pooling Criteria

Select the pooling criteria to use for this server system pool.

Resilience criteria:

□ Only add hosts capable of live virtual server relocation

Note: When adding hosts that contain existing virtual servers, the existing virtual servers will be excluded from server system pool management. These virtual servers will still run on the host, but not be managed by the server system pool.

Learn about server system pool capabilities

To set up manual mobility when using VMControl version 2.4.1, follow these steps:

Procedure

1. Ensure resiliency is enabled and automatic relocation disabled.
2. Copy the `vsi_service_config.properties` file from the META-INF folder in the `com.ibm.ensemble.local.mgmt_<version>.jar` to the `/lwi/conf/overrides/` folder.
3. Edit the `vsi_service_config.properties` properties file with the following line:

   ```
   vsi.placementoptimizer.deploys.evacuation.no.relocation = 1
   ```
4. Save the file and continue with creating the system pool.

Enabling retry of HMC commands

VMControl enables a retry feature that allows VMControl to retry an HMC command if it fails. This retry feature must be configured in order for it to be enabled.

About this task

To enable this feature, follow these steps:

Procedure

1. Open the `/opt/ibm/director/data/VSMPower.properties` file.
2. Add the following properties to the file.

   ```
   CommandCallRetries=5
   CommandCallRetryDelay=30
   ```

   With these properties set, if an HSCL3205 error is detected, the failing command is retried using the configured number of retries and the configured delay in seconds between retries. Using the properties as specified in the example, the failing command has 4 retries with 30 second wait in between retries.
3. Save and close the `/opt/ibm/director/data/VSMPower.properties` file.

VMware prerequisite installation

The IBM SmartCloud Entry is compatible with existing installations of VMware vSphere managed by the VMware vCenter. Ensure that the VMware vCenter Server product is installed, operational, and managing a VMware vSphere environment.

For more information about supported VMware distributions, see "VMware prerequisites" on page 11.

The configuration of the VMware products is outside the scope of this document. Refer to the product documentation for configuration and troubleshooting instructions.

Links

- VMware vCenter Server website at http://www.vmware.com/products/vcenter-server/overview.html.
- VMware vSphere website at http://www.vmware.com/products/vsphere/overview.html.
- VMware Documentation website at http://www.vmware.com/support/pubs/.

IBM SmartCloud Entry supports only Windows and Linux guest operating systems, which are supported by vCenter and ESXi and allow guest customizations. For more information, see the following resources:

- VMware Compatibility Guide for Guest Operating Systems
- Guest Operating Customization Guide

Customization of certain Microsoft Windows operating systems requires Microsoft Sysprep Tools. Refer to *Installing the Microsoft Sysprep Tools* section of the Developer's Setup Guide PDF at http://www.vmware.com/support/developer/vc-sdk/visdk41pubs/vsp41_developerssetupguide.pdf for detailed instructions about obtaining the Sysprep Tools and where to store the tools on the vCenter Servers file systems.

Configuration considerations for VMware

- Use DRS-enabled clusters for advanced placement

  Allow vCenter to place the user workload on the best host machine by using a DRS-enabled cluster within vCenter and setting the appliance target to use the cluster or a resource pool that is defined in the cluster. This allows vCenter to manage the available host resources. Otherwise, the appliance target is an individual host machine or a resource pool on a host machine.
- Place vCenter server and IBM SmartCloud Entry server on the same network.

  For best performance, it is recommended the vCenter server and the IBM SmartCloud Entry server are on the same network.

Microsoft Hyper-V prerequisite installation

IBM SmartCloud Entry, using OpenStack technologies, is compatible with existing installations of Microsoft Hyper-V hypervisor. Ensure that the Microsoft Hyper-V hypervisor is operational and managing environments.

For more information about supported Hyper-V distributions, see "IBM SmartCloud Entry Hyper-V Agent Installation Prerequisites" on page 63.

The management of Microsoft Hyper-V hypervisor is outside the scope of this document. Refer to the product documentation for troubleshooting instructions. For more information about setting up and configuring Microsoft Hyper-V as a managed hypervisor, see Chapter 11, "Installing the IBM SmartCloud Entry Hyper-V Agent," on page 63.

Database prerequisites (optional)

The first time IBM SmartCloud Entry is deployed to your server, it automatically installs the IBM SmartCloud Entry database. This database holds all the information known to IBM SmartCloud Entry including configuration, users, images, instances, events, and so on.

The default database used by IBM SmartCloud Entry is a Derby database for which there are *no* prerequisite installation steps required. The default Derby database is created inside the IBM SmartCloud Entry home directory.

Downloading and installing DB2

IBM SmartCloud Entry also supports the use of IBM DB2 as the database application.

For information about how to download, install, and configure DB2, refer to its product documentation. Additionally, see the DB2 for Linux, UNIX and Windows website at http://www.ibm.com/software/data/db2/linux-unix-windows/.

Note: IBM SmartCloud Entry does not support SSL connections to DB2.

After DB2 is successfully installed and configured, create a DB2 database for IBM SmartCloud Entry and configure IBM SmartCloud Entry to use it.

Creating a DB2 database for IBM SmartCloud Entry

While the default database used by IBM SmartCloud Entry is a Derby database, you can create a DB2 database to use.

About this task

The following steps are required to create a DB2 database for IBM SmartCloud Entry use.

Procedure

1. Start the DB2 Control Center.
2. Navigate to the location of the new database.
3. Right-click and select Create Database.
4. Complete the fields on the Create Database Wizard.

   Note:

   - Be sure to specify at least 8K for the default bufferpool and table space size.
   - Check to use the database path as a storage path.
   - Change to Unicode (UTF-8) for the Code set.
5. Select Finish.
6. Create or edit the *database.properties* file in the IBM SmartCloud Entry home directory as described in the “Configuring database” on page 82 section.
7. Start the database by right-clicking it and selecting Start.

Chapter 6. Installing IBM SmartCloud Entry

The IBM SmartCloud Entry installer supports three installation types: console, graphical (swing), and silent.

The installer supports three operating systems: 64-bit AIX on Power®, 64-bit Linux, and Windows. For AIX and Linux, the default installation type is console and the default installation type for Windows is graphical. To install IBM SmartCloud Entry using a non-default installation type, start the installer from the command line and run `-i <install type>` where `<install type>` is `console`, `silent`, or `swing`.

As an alternative to using the IBM SmartCloud Entry installer, on System x® systems you can deploy the IBM SmartCloud Entry virtual appliances for System x. For more information, see Chapter 10, "Deploying IBM SmartCloud Entry Virtual Appliances for System x," on page 47.

New installation on Windows

To install IBM SmartCloud Entry on Windows, follow the steps outlined in these topics.

Graphical installation (default)

You can complete the installation through a GUI, if you prefer.

Procedure

1. Go to the location of the Windows installer and double-click the installer icon.
2. On the first screen, select the language that you want the installer displayed in from the drop-down menu and click **OK**.

   Note:
   - If you see an error message similar to `Executing java permission denied`, verify you are using the correct installer for your operating system.
   - If you see Windows error 183, you are using am unsupported 32-bit operating system.
3. On the Introduction screen, read the introduction for information about the installer and click **Next**.
4. On the License Agreement window, read the contract and accept the license. Click **Next**.
5. On the Choose Shortcut Location window, select the check boxes next to the locations where you want a IBM SmartCloud Entry link and then click **Next**.
6. To choose the location for your installation, click **Choose** on the Choose Install Folder window, specify your chosen location, and click **Next**.

   Note:
   - The install path cannot contain non-English characters.
   - In IBM SmartCloud Entry 2.2, this folder was called `Starter Kit for Cloud`. Because later releases of IBM SmartCloud Entry install into the `SmartCloud Entry` folder, you do not have to uninstall your IBM SmartCloud Entry 2.2 version. Instead, you can install the new version into the same directory for a side by side installation.
7. To select the location of your property files, on the Choose Property File Install Folder window, click **Choose** and click **Next**.

   Note: The install path cannot contain non-English characters.
8. Review your selected options on the Pre-Installation Summary window. If you are satisfied with your selections, click **Next**.

9. After the installation is finished, the Install Finished window opens.

   You have three options:

   - You can follow the installer to configure important properties.
   - You can use the installer to migrate the property files and database from a previous release.
   - You can manually migrate the configuration property files and data from a previous release at a later time.

   Click **Next** after making your selection and complete one of the following steps if you chose to migrate or configure the property file information:

   Note: The property files must be configured in your environment before you can use IBM SmartCloud Entry.

   - If you selected to configure the property files with the installer, the Add Configuration Values window opens. If you selected to configure the property files, the Add Configuration Values window opens. Enter the host name and the configured user name and password used to communicate with the host, and then click **Next**.
   - If you selected to use the installer to migrate the configuration and database, complete the following steps:
     a. Stop the IBM SmartCloud Entry if it is running.
     b. Locate the installation folder of the installation you want to migrate.

     The installer will start the newly installed IBM SmartCloud Entry instance and migrate the configuration and database from the previous installation.

     Note: You cannot migrate a DB2 database using the installer. To migrate your DB2 database, see "Migrating your data" on page 36.

     After the migration is complete, see"Migrating your configuration" on page 35 for more information about the files and values that must be manually migrated.
   - To manually configure your properties files, see "Configuring local authentication" on page 80 and "Configuring common cloud properties" on page 83.
   - To manually migrate your configuration and database, see "Migrating your configuration" on page 35.

Console installation

You can complete the installation through a console, if you prefer.

Procedure

1. Click **Start** and then select **Run**.
2. In the run window, type `cmd` and click **OK**.
3. In the console window, navigate to the windows installer and run the following command:

   ```
   sce310_windows_installer.exe -i console
   ```
4. On the Choose Locale screen, choose the language for the installer by typing the number corresponding to your chosen language and pressing Enter. If your preferred language is the default, press Enter.

   Note:

   - If you see an error message similar to `Executing java permission denied`, verify that you are using the correct installer for your operating system.
   - If you see Windows error 183, you are using am unsupported 32-bit operating system.
5. On the Introduction screen, read the information about the installer and press Enter.
6. On the License Agreement screen, read the contract and accept the license by entering Y.

7. Choose your location for the links to IBM SmartCloud Entry. To choose any combination of locations, separate each number with a comma.
8. On the Choose Install Folder screen, press Enter to accept the default location. To choose a different location for the application files, type in the full path to that folder and press Enter.

   Note:
   - The installation path cannot contain non-English characters.
   - In IBM SmartCloud Entry 2.2, this folder was called `Starter Kit for Cloud`. Because later releases of IBM SmartCloud Entry install into the `SmartCloud Entry` folder, you do not have to uninstall your IBM SmartCloud Entry 2.2 version. Instead, you can install the new version into the same directory for a side by side installation.
9. On the Choose Property File Install Folder screen, press Enter to accept the default location. To choose a different location for the property files, type in the full path to that folder and press Enter.

   Note: The installation path cannot contain non-English characters.
10. Review your selected options on the Pre-Installation Summary screen. If you are satisfied with your selections, press Enter.
11. When the installation is complete, the Install Finished window opens.

    You have three options:
    - You can follow the installer to configure important properties.
    - You can use the installer to migrate the property files and database from a previous release.
    - You can manually migrate the configuration property files and data from a previous release later.

    Click **Next** after making your selection and complete one of the following steps if you chose to migrate or configure the property file information:

    Note: The property files must be configured in your environment before you can use IBM SmartCloud Entry.
    - If you selected to configure the property files, the Add Configuration Values window opens. Enter the host name and the configured user name and password that is used to communicate with the host, and then click **Next**.
    - If you selected to migrate the configuration and database, complete the following steps:
      a. Stop the IBM SmartCloud Entry if it is running.
      b. Locate the installation folder of the installation you would like to migrate.

      The installer starts the newly installed IBM SmartCloud Entry and migrates the configuration and database from the previous installation.

      Note: The migration of a DB2 database is not supported in the installer. For more information about migrating a DB2 database, see “Migrating your data” on page 36.

      When the migration is complete, see “Migrating your configuration” on page 35 for more information about the files and values that must be manually migrated.
    - To manually configure your properties files, see “Configuring local authentication” on page 80 and “Configuring common cloud properties” on page 83.

      To manually migrate your configuration and database, see “Migrating your configuration” on page 35.

Silent installation

Create a IBM SmartCloud Entry silent installation response file and use it to install Windows.

About this task

To create a silent installation response file, follow either“Console installation” on page 24 or“Graphical installation (default)” on page 23 on Windows. On the final screen, you can create a silent installation response file. Creating a silent installation response file creates a property file that is called `installer.properties` in the installation location.

To install Windows by using a silent installation response file, follow these steps:

Procedure

1. Open the response file and double check all of the properties. Notice that the passwords are not in the file. Also, notice that all paths have "\\" instead of a single "\". Make any updates and then save the file.
2. Press Start and then Run.
3. In the run prompt, type `cmd` and press Enter.
4. A console window opens. In the console window, navigate to the Windows installer.
5. Run the installer with the command `sce310_windows_installer.exe -i silent -f <response file location>`, where `<response file location>` is the path to the response file, which defines the installation.

   Note:
   - If you see an error message similar to `Executing java permission denied`, verify that you are using the correct installer for your operating system.
   - If you see Windows error 183, you are using am unsupported 32-bit operating system.
   - If you have spaces in a directory name, then you must put double quotation marks around it as shown in the following example:
     ```
     sce310_windows_installer.exe -i silent -f "c:\My Directory\installer.properties"
     ```

New installation on Linux or AIX

To install IBM SmartCloud Entry on 64-bit Linux or 64-bit AIX on Power, follow the steps outlined in these topics.

Console installation (default)

You can complete the installation through a console, if you prefer.

Procedure

1. Go to the location of the Linux or AIX installer and run the installer with the following command that is appropriate for your environment:

   Important: You need root authority to run the installer.
   - On AIX on Power, run: `./sce 310_aix_installer.bin`
   - On Linux, run: `./sce310_linux_installer.bin`
2. On the Choose Locale screen, choose the language for the installer by typing the number corresponding to your chosen language and pressing Enter. If your preferred language is the default, press Enter.

   Note:
   - If you see an error message similar to `Executing java permission denied`, verify that you are using the correct installer for your operating system.
   - If you see Windows error 183, you are using am unsupported 32-bit operating system.

3. On the Introduction screen, read the information about the installer and press Enter.
4. On the License Agreement screen, read the contract and accept the license by entering Y.
5. On the Choose Link Location screen, choose your location for the links to IBM SmartCloud Entry. Complete one of the following steps to choose your location:
   - To choose any combination of locations, separate each number with a comma.
   - To choose the default location, press Enter.
   - To choose your home directory, type 2 and press Enter.
   - To choose another location, type 3, press Enter, and then type in the full path of your selected location.
   - To not install any links, type 4 and press Enter.

     Note: To run IBM SmartCloud Entry without links, run the **`sce`** command in the application installation folder.
6. On the Choose Install Folder screen, press Enter to accept the default location. To choose a different location for the application files, type in the full path to that folder and press Enter.

   Install locations by release:
   - IBM SmartCloud Entry 2.2: `SKC`
   - IBM SmartCloud Entry 2.3: `SCE23`
   - IBM SmartCloud Entry 2.4: `SCE24`
   - IBM SmartCloud Entry 3.1: `SCE31`

   Note:
   - The installation path cannot contain non-English characters.
   - You do not have to uninstall previous releases of IBM SmartCloud Entry. Instead, you can install the new version into the same directory for a side by side installation.
7. On the Choose Property File Install Folder screen, press Enter to accept the default location. To choose a different location for the property files, type in the full path to that folder and press Enter.

   Note: The installation path cannot contain non-English characters.
8. Review your selected options on the Pre-Installation Summary screen. If you are satisfied with your selections, press Enter.
9. When the installation is finished, the Install Finished window opens.

   You have three options:
   - You can migrate the property files and database from a previous release.
   - You can follow the installer to configure important properties.
   - You can manually perform a migration or manually upgrade the property files.

   Click **Next** after you make your selection and complete one of the following steps if you chose to migrate or configure the property file information:

   Note: The property files must be configured in your environment before you can use IBM SmartCloud Entry.
   - If you selected to configure the property files, the Add Configuration Values window opens. Enter the host name and the configured user name and password that is used to communicate with the host, and then click **Next**.
   - If you selected to migrate the configuration and database, complete the following steps:
     a. Stop the IBM SmartCloud Entry if it is running.
     b. Locate the installation folder of the installation you would like to migrate and run it.

     The installer starts the newly installed IBM SmartCloud Entry and migrate the configuration and database from the previous installation.

Note: The migration of a DB2 database is not supported in the installer. For more information about migrating a DB2 database, see "Migrating your data" on page 36.

When the migration is complete, see "Migrating your configuration" on page 35 for more information about the files and values that must be manually migrated.

- To manually configure your properties files, see "Configuring local authentication" on page 80 and "Configuring common cloud properties" on page 83.

  To manually migrate your configuration and database, see "Migrating your configuration" on page 35.

Graphical installation

You can complete the installation through a GUI, if you prefer.

Procedure

1. Go to the location of the Linux or AIX installer and run the installer with the following command that is appropriate for your environment:
   - On AIX on Power, run: `./sce310_aix_installer.bin -i swing`
   - On Linux, run: `./sce310_linux_installer.bin -i swing`
2. On the first screen, select the language that you want to use for the installer from the drop-down menu and click **OK**.

   Note:
   - If you see an error message similar to `Executing java permission denied`, verify that you are using the correct installer for your operating system.
   - If you see Windows error 183, you are using am unsupported 32-bit operating system.
3. On the Introduction screen, read the introduction for information about the installer and click **Next**.
4. On the License Agreement window, read the contract and accept the license. Click **Next**.
5. On the Choose Shortcut Location window, select the check boxes next to the locations where you want a IBM SmartCloud Entry link and then click **Next**.
6. To choose the location for your installation, click **Choose** on the Choose Install Folder window, specify your chosen location, and click **Next**.

   Install locations by release:
   - IBM SmartCloud Entry 2.2: `SKC`
   - IBM SmartCloud Entry 2.3: `SCE23`
   - IBM SmartCloud Entry 2.4: `SCE24`
   - IBM SmartCloud Entry 3.1: `SCE31`

   Note:
   - The installation path cannot contain non-English characters.
   - You do not have to uninstall previous releases of IBM SmartCloud Entry. Instead, you can install the new version into the same directory for a side by side installation.
7. To select the location of your property files, on the Choose Property File Install Folder window, click **Choose** and click **Next**.

   Note: The installation path cannot contain non-English characters.
8. Review your selected options on the Pre-Installation Summary window. If you are satisfied with your selections, click **Next**.
9. When the installation is complete, the Install Finished window opens.

   You have three options:
   - You can migrate the property files and database from a previous release.

- You can follow the installer to configure important properties.
- You can manually perform a migration or manually upgrade the property files.

Click **Next** after you make your selection and complete one of the following steps if you chose to migrate or configure the property file information:

Note: The property files must be configured in your environment before you can use IBM SmartCloud Entry.

- If you selected to configure the property files, the Add Configuration Values window opens. Enter the host name and the configured user name and password that is used to communicate with the host, and then click **Next**.
- If you selected to migrate the configuration and database, complete the following steps:
  a. Stop the IBM SmartCloud Entry if it is running.
  b. Locate the installation folder of the installation you would like to migrate.

  The installer starts the newly installed IBM SmartCloud Entry and migrates the configuration and database from the previous installation.

  Note: The migration of a DB2 database is not supported in the installer. For more information about migrating a DB2 database, see "Migrating your data" on page 36.

  When the migration is complete, see "Migrating your configuration" on page 35 for more information about the files and values that must be manually migrated.
- To manually configure your properties files, see "Configuring local authentication" on page 80 and "Configuring common cloud properties" on page 83.

  To manually migrate your configuration and database, see "Migrating your configuration" on page 35.

Silent installation

Create a IBM SmartCloud Entry silent installation response file and use it to install AIX or Linux.

About this task

To create a silent installation response file, follow either "Console installation (default)" on page 26 or "Graphical installation" on page 28 on Linux or AIX. On the final screen, you can create a silent installation response file. Creating a silent installation response file creates a property file that is called `installer.properties` in the installation location.

To install AIX or Linux using a silent installation response file, follow these steps:

Procedure

1. Open the response file and check all of the properties. Note that all the passwords are not in the file. Make any updates and then save the file.
2. Go to the location of the Linux or AIX installer and run the installer with the following command that is appropriate for your environment:
   - On AIX on Power, run: `./sce310_aix_installer.bin -i silent -f <response file location>`, where `<response file location>` is the path to the response file, which defines the installation.
   - On Linux, run: `./sce310_linux_installer.bin -i silent -f <response file location>`, where `<response file location>` is the path to the response file, which defines the installation.

   Note:

   - If you see an error message similar to `Executing java permission denied`, verify that you are using the correct installer for your operating system.
   - If you see Windows error 183, you are using am unsupported 32-bit operating system.

The IBM SmartCloud Entry installation is complete.

Applying fixes and updates for IBM SmartCloud Entry

Updates for IBM SmartCloud Entry provide fixes to the product. IBM SmartCloud Entry has a Command Line Interface (CLI) that is used to update the application. The CLI is available from the OSGi console that opens when the application starts.

About this task

Note: If you installed IBM SmartCloud Entry by deploying anIBM SmartCloud Entry for System x appliance, see “Performing support and maintenance tasks on the IBM SmartCloud Entry for System x appliance” on page 61 for instructions to apply fixes and updates to your appliance.

Depending on where you chose to download the update package, you either access a URL-based repository for remotely installing packages or local file system directory repository on the system running IBM SmartCloud Entry. Updates using remote (URL-based) or local file system (directory) repositories are the same except for the format of the repository that is specified on the CLI. URL-based repositories are of the form `http://UPDATE_REPOSITORY`, while local file system (directory) repositories have the form file: `PATH_TO_DIRECTORY`. When using a local file system repository, you must use forward slashes in the full path to the local directory.

Note: Before you install a fix pack or upgrade IBM SmartCloud Entry, back up your `skc.ini` file to a safe location. After you install the fix pack or finish upgrading, replace the `skc.ini` file with your backup version.

The following update commands are available from the CLI:

`version`
Returns the current product version.

`showrepos`
Returns a list of the update repositories that are associated with the product.

`addrepo [url]`
Adds a repository to the product from the file or remote URL.

`delrepo [url]`
Removes a repository (* for all repositories) from the product.

`checkupdates`
Returns a list of the current updates available.

`installupdates`
Installs the available updates to the product.

`updatetimestamps`
Returns a list of the product update timestamps.

`rollbackupdates [timestamp]`
Rolls back to the timestamp. If no timestamp is given the rollback is to the previous timestamp.

To download and install fixes for IBM SmartCloud Entry, follow these steps:

Procedure

1. Open your browser to IBM Support Fix Central at http://www-933.ibm.com/support/fixcentral/
2. Select **Select product**.
3. Select **Other Software** for the Product Group.
4. For the Product, select IBM SmartCloud Entry version 3.1.

5. Select **All** for the Installed Version.
6. Select **All** for the Platform and select **Continue**.
7. Identify fixes by selecting **Browse** for fixes and select **Continue**.
8. Select the specific fix that you want and select **Continue**.
9. Authenticate to the Fix Central server to demonstrate entitlement.
10. Select the method that you want to use to download the fix and select **Continue**.
11. Store the update in a repository that is available remotely or locally on the system that is running IBM SmartCloud Entry.
12. Extract the compressed file to the disk drive of the system in a temporary directory.
13. In the IBM SmartCloud Entry OSGi command console, use the **`showrepos`** command to list the repositories that are associated with the IBM SmartCloud Entry. For example:

    ```
    osgi> showrepos
    Metadata repositories:
    Artifacts repositories:
             file:/C:/Users/IBM_ADMIN/.eclipse/207580638/p2/org.eclipse.
    equinox.p2.core/cache/
    ```

14. If the repository that is storing the extracted files is not available, use the **`addrepo`** command to add that repository.

    ```
    osgi> addrepo file:C:/temp/myFixPack
    SKC update repository added
    ```

15. Install the updates by using the **`installupdates`** command.

    ```
    osgi> installupdates
    SKC updates to install:
            com.ibm.cfs.product 2.2.0.0-20110831 ==> com.ibm.cfs.product 2.2.0.1-20111225
    SKC update done
    ```

16. When the update is complete, activate the changes by using the **`close`** command to end the OSGi session, then restarting IBM SmartCloud Entry.

    ```
    osgi> close
    ```

17. If you want to remove the updates and return to a previous configuration of IBM SmartCloud Entry, follow these steps:
    a. If you have not yet restarted IBM SmartCloud Entry after applying an update, you must close your OSGi session and restart IBM SmartCloud Entry before you can roll back the changes.

    b. Determine the timestamp of the update by running the **`updatetimestamp`** command:

    ```
    osgi> updatetimestamps
    Update Tim-stamps:
    1316152892234: Fri Sep 16 02:01:32 EDT 2011
    1316152892237: Fri Sep 16 02:01:32 EDT 2011
    1316152893623: Fri Sep 16 02:01:33 EDT 2011
    1316152894203: Fri Sep 16 02:01:34 EDT 2011
    1316193855750: Fri Sep 16 13:24:15 EDT 2011
    1316193903656: Fri Sep 16 13:25:03 EDT 2011
    ```

    c. Use the **`rollbackupdates`** command to remove the updates.

    ```
    rollbackupdates 1316193903656
    ```

    If you do not provide a timestamp to the **`rollbackupdates`** command, the last timestamp is used.

    d. When the rollback is complete, activate the changes by using the **`close`** command to end the OSGi session, then restarting IBM SmartCloud Entry.

IBM SmartCloud Entry for Cloud SSL configuration (optional)

The IBM SmartCloud Entry ships a self-signed certificate for SSL communication between a client machine, such as a web browser, and the IBM SmartCloud Entry server. This certificate is stored in *<home directory>* `/.keystore` file.

This self-signed certificate is shipped for testing purposes only. It is not associated with a qualified host and domain name. Additionally, it is self-signed so a security warning is displayed when accessing the host using https. To use SSL configuration in production, create a different self-signed or CA issued certificate that is designated specifically for the qualified host. Additionally, the keystore password must be changed or another keystore must be used to contain this certificate with a secure password. The new passwords would then be used in the following `server.properties` file configuration example.

To export a certificate to be used by clients, run the following command from the .SCE31 directory:

```
"<jre path>/keytool" -export
-v -alias SKC -file SKC.cer -keystore .keystore -storepass cfs4ibm
```

Notes:

- In order for this command to run properly, the `Java/bin` directory must be added to the system `%PATH%` variable.
- **`keytool`** is a key and certificate management utility that is included with Java™ SE 6.0.

After this certificate is imported into a client, the client can communicate with IBM SmartCloud Entry by using the trusted certificate with no additional user intervention required. If the import is not done, the client, such as a browser, might prompt the user to verify it and confirm that the certificate is trusted. After you confirm that you accept the risk of the certificate, you will be able to use SSL.

SSL is enabled on the server by configuring the `server.properties` file in the IBM SmartCloud Entry home directory.

```
# HTTP server port
org.osgi.service.http.port=8080

# Flag to enable/disable HTTPS
org.eclipse.equinox.http.jetty.https.enabled=false

# HTTPS port
org.eclipse.equinox.http.jetty.https.port=8443

# SSL password
org.eclipse.equinox.http.jetty.ssl.password=cfs4ibm

# Keystore password
org.eclipse.equinox.http.jetty.ssl.keypassword=cfs4ibm

# The full path location of the keystore
org.eclipse.equinox.http.jetty.ssl.keystore=/.skc/.keystore

# The SSL protocol
org.eclipse.equinox.http.jetty.ssl.protocol=SSL_TLS
```

The org.eclipse.equinox.http.jetty.ssl.protocol property is *SSL_TLS* if running on an IBM JRE. The property is *TLS* if running on a Sun or Oracle JRE.

If it is necessary for the protocol to be only SSL, ensure the org.eclipse.equinox.http.jetty.http.enabled property is configured to false.

Restart the server after changing the `server.properties` file. With the server running, point your client to `https://`*`system`*`:8443/cloud/api/users` to test it. Depending on whether you imported the certificate from above, you might be prompted to accept the certificate.

Creating a new certificate for your host

You can use the **keytool** tool to create a self-signed certificate for the host you are deploying IBM SmartCloud Entry on or to create a certificate signing request (CSR) to send to a certificate authority (CA) to get a CA-issued certificate that is trusted by clients automatically.

For example, to generate a new keystore with specific customer information, use the following command:

```
keytool -genkey -dname "CN=cloud.ibm.com, OU=Cloud Services, O=IBM, L=RTP, S=NC, C=US"
-alias SKC -keystore .keystore -keyalg RSA -keysize 1024
```

CN Specifies the customers domain.

OU Specifies the organization within the customer's company.

O Specifies the company.

L Specifies the city of the company location.

S Specifies the state where that city resides.

CB Specifies the country.

To generate a certificate signing request from the keystore, run the following command:

```
keytool -certreq -alias SKC -keystore .keystore -file NewCertSignRequest.csr
```

To import the trusted certificate (.cer) file, run this command:

```
keytool -import -trustcacerts -alias SKC -file ./TrustedCertificate.cer -keystore .keystore
```

See the **keytool** documentation for your JRE for instructions. For the IBM JRE, the instructions are available at http://www.ibm.com/developerworks/java/jdk/security/60/secguides/keytoolDocs/keytool.html.

Note: When the CA is not trusted by clients automatically and you are attempting to access IBM SmartCloud Entry using https protocol, an exception is encountered that says the connection is untrusted. You must confirm that the risks are understood and must add an exception to continue. Even with a trusted certificate, when using Internet Explorer, you are likely to run into a similar exception.

Connecting using SSH

If you use a secure shell (SSH) protocol to communicate with your IBM SmartCloud Entry server, SSH encrypts authentication traffic going to and from the server.

To further minimize security risks when connecting using OpenSSH, change the OpenSSH daemon configuration file so that the line containing `Protocol` is changed to 2. Anything less than 2 is more susceptible to attack.

Chapter 7. Migrating IBM SmartCloud Entry

This section describes different methods for migrating IBM SmartCloud Entry to a new release.

There are several options for migrating IBM SmartCloud Entry to a new release:
- Manually migrating to a new release
- Migrating from one system to another
- Migrating to a version 3.1 IBM SmartCloud Entry for System x virtual appliance
- Migrating a Derby database to a DB2 database

Migrating to a new release

You can migrate your IBM SmartCloud Entry configuration when you are installing a new release.

To migrate data and configuration files that are not migrated by the installer or to manually migrate your data and configurations, follow the instructions in these topics. When you migrate data in IBM SmartCloud Entry you must migrate sequentially; you cannot skip a version. For example, if you want to migrate IBM SmartCloud Entry version 2.3 to version 3.1, you need to migrate from version 2.3 to version 2.4 first. Before you migrate to the latest version, ensure that all available fix packs are applied. Then, migrate from IBM SmartCloud Entry version 2.4 (with fix packs) to version 3.1.

To migrate IBM SmartCloud Entry to a new release, take the following general steps:
- Migrate your configuration
- Migrate your data
- (Optional) Manually migrate any remaining configuration files

Migrating your configuration

When you migrate to a new version of IBM SmartCloud Entry, you can choose to migrate all of your preferences from one set of configuration files to the new set.

To migrate your preferences from one set of configuration files to the new set, use the following OSGi command:

```
migrateConfig [source directory]
```

where *source directory* is the location of the previous IBM SmartCloud Entry release configuration files.

Running this command migrates the following configuration files:
- `cfs.keystone`
- `ldap.xml`
- `deployment.properties`
- `authentication.properties`: `admin.username`, `admin.password`, and `admin.name` should not be updated.
- `email.properties`
- `messaging.properties`
- `metering.properties`
- `billing.properties`
- `web.properties`
- `*.jks`
- `products/*.xml`

Example

To migrate configuration files from a previous version, run the following command:

```
migrateConfig C:\oldSKC\.skc
```

Migrating your data

When you are migrating to a new version of IBM SmartCloud Entry, you can choose to migrate data from your previous database.

Before you begin

To prepare for the data migration, follow these steps:

1. Ensure that the target database exists.
2. In your browser, log out and close all open IBM SmartCloud Entry windows.

Procedure

To migrate your data, use the following OSGi command:

```
upgradeDatabase 'DB2_Path' 'DB2_User_Name' 'DB2_password'
```

where *DB2_Path* is the path of the DB2 database, *DB2_User_Name* is the name of the DB2 administrator, and *DB2_password* is the password for the DB2 administrator.

Note: *DB2_User_Name* and *DB2_password* are only needed when migrating data from a DB2 database.

Notes:

- The **upgradeDatabase** command supports only major versions of databases.
- The source database must be Derby or DB2.
- Only approved requests can be migrated, while others such as pending requests, rejected requests, and withdrawn requests cannot be migrated. If the approved requests related instances have been deleted, they cannot be migrated either.
- If any errors occur during migration, renew the target database and run the **upgradeDatabase** command again.

Results

You can see migration details in the console.

Example

- To migrate your data from a Derby database, run the following command:
  ```
  upgradeDatabase 'C:\oldSKC\.skc\'
  ```
- To migrate your data from a DB2 database, run the following command:
  ```
  upgradeDatabase '//localhost:50001/skc''db2admin' 'db2passwd'
  ```

What to do next

You must restart IBM SmartCloud Entry after migration.

Migrating configuration manually

Some configuration information must be migrated manually.

This configuration information includes:

- Network configuration
- Security relevant files
- Logging.properties file
- skc.ini file

Note: When migrating configuration information for a Microsoft Windows 2008 installation, you must manually configure the cloud connection.

Migrating from one system to another

You can migrate your IBM SmartCloud Entry configuration from one system to another system.

About this task

Note: Migrating a configuration from one system to another replaces the configuration on the target system.

To migrate IBM SmartCloud Entry from one system to another, follow these steps:

Procedure

1. Shut down IBM SmartCloud Entry on the target system.
2. Copy the `.SCE31` directory from the source system to the target system, overwriting the `.SCE31` directory on the target system.
3. Update the directory path in the `logging.properties` file to the following:
   ```
   java.util.logging.FileHandler.pattern=/home/sysadmin/.SCE31/logs/skc-%g.log
   ```
4. Update the directory path in the `server.properties` file to the following:
   ```
   org.eclipse.equinox.http.jetty.ssl.keystore=/home/sysadmin/.SCE31/.keystore
   ```
5. Use the appropriate option on the **sceappmgr** menu to generate a new SimpleToken on the target system.
6. Start IBM SmartCloud Entry on the target system.

   The configuration from the source system is now available on the target system.

Migrating from version 2.4 to a version 3.1 appliance

You can migrate IBM SmartCloud Entry version 2.4 to a version 3.1 appliance.

About this task

To migrate to a version 3.1 appliance, follow these steps:

Procedure

1. Copy the version 2.4 version on this system to the following directory:
   ```
   /home/sysadmin/
   ```
   Use one of the following methods to copy this information:
   - scp

     For example, from the remote host where the previous version of IBM SmartCloud Entry 2.4 is installed, run a command similar to the following:
     ```
      scp -r /root/.SCE24 sysadmin@<Appliance IP>:/home/sysadmin/
     ```
     where *Appliance IP* is the IP address of the appliance.
   - winscp

- sftp

  For example, you could compress the directory on the remote system, use SFTP to copy the compressed directory to the appliance and then extract it, as follows:

  ```
  zip -rv SCE24.zip .SCE24
  sftp sysadmin@Appliance IP
  put SCE24.zip
  quit
  ```

  and then

  ```
  ssh sysadmin@Appliance IP
  unzip SCE24.zip
  exit
  ssh sysadmin@Appliance IP
  ```

  where *Appliance IP* is the IP address of the appliance.
- mount

  Note: You can also use FTP to copy files to the appliance, but you cannot use FTP from another host system.

2. Use the appropriate option on the **sceappmgr** menu to migrate from version 2.4 to a version 3.1 appliance.

   This migrates the cloud connections, integrates the properties files, and updates the database.

Migrating a Derby database to DB2 database

Use the **migratedatabase** command to move the IBM SmartCloud Entry database from an embedded Derby database to an external DB2 database. Migrating to an external DB2 database can improve scaling, performance, and production level data store.

To prepare for the migration process, follow these steps:

1. Ensure that the DB2 database exists and is empty. For instructions about how to create the database, see “Creating a DB2 database for IBM SmartCloud Entry” on page 22.
2. Configure IBM SmartCloud Entry to use DB2. For more information, see “Configuring database” on page 82.
3. In your browser, log out and close all opened IBM SmartCloud Entry windows.

To migrate the current database to the DB2 database, use the following OSGi command:

```
migrateDatabase source_directory
```

where *source_directory* is the property file location. You can see migration details in the console. It is not necessary to restart IBM SmartCloud Entry after migration.

Example: Migrating from a Derby database to a DB2 database

Migrate the Derby database to a DB2 database by running the following command:

```
migrateDatabase 'C:\oldSCE24\.SCE24\'
```

Notes:

- Only approved requests can be migrated, while others such as pending requests, rejected requests, and withdrawn requests cannot be migrated. Approved requests related instances that have been deleted cannot be migrated.
- If any errors occur during migration, renew DB2 first and try running the **migrateDatabase** command again.

- To free up the space that is occupied on IBM SmartCloud Entry server, the **migrateDatabase** command clears the Derby database following the migration. Create a backup of the Derby database before migration.
- During migration, invoice IDs might change.

Chapter 8. Starting and stopping IBM SmartCloud Entry

The following steps are required for starting IBM SmartCloud Entry on Windows, AIX, and Linux.

Note: When starting or restarting IBM SmartCloud Entry on a high scale cloud, the synchronization between IBM SmartCloud Entry and the cloud might take longer than expected. This resynchronization might cause operations such as deploying, deleting, or resizing an instance to be delayed or even fail. Wait for the synchronization to complete before you attempt these actions.

Starting and stopping IBM SmartCloud Entry on Windows

To start IBM SmartCloud Entry, navigate to **All Programs** > **IBM SmartCloud Entry 3.1** > **SmartCloud Entry**. Alternatively, you can double-click the **SmartCloud Entry 3.1** icon that might be installed on your desktop. In 10 to 20 seconds, the server is available and you can access IBM SmartCloud Entry by opening http://localhost:8080/cloud/web/index.html in a supported browser.

Note: The host name **localhost** and port **8080** are the default host and port names. Substitute the appropriate values for your environment if necessary.

To stop IBM SmartCloud Entry, shut down the IBM SmartCloud Entry instance by closing the window or by using Ctrl-C to end it.

If the IBM SmartCloud Entry instance was started with an OSGi console running in the background, you might have to telnet to it with the correct port to access the console. Refer to OSGi console for more details. From the OSGi console, type `shutdown` to stop IBM SmartCloud Entry and then `exit` to exit immediately. Exit IBM SmartCloud Entry before restarting.

Starting and stopping IBM SmartCloud Entry on Linux or AIX

The IBM SmartCloud Entry installation on Linux or AIX can be started by the root user or by users who are members of the sce group. By default no users are part of the sce group. Only the root user can add more users to the sce group on Linux or AIX. The sce group is created as part of the IBM SmartCloud Entry installation.

To start IBM SmartCloud Entry on Linux or AIX, navigate to the link location specified during installation. By default this location is the `/usr/bin` directory. From the link directory, run the file that is called *SCE_31* or *runSCE_31*. When the start is complete, the server is available and you can access IBM SmartCloud Entry by opening `http://localhost:8080/cloud/web/index.html` in a supported browser.

Note: The host name **localhost** and port **8080** are the default host and port names. Substitute the appropriate values for your environment if necessary.

To stop IBM SmartCloud Entry, shut down the IBM SmartCloud Entry executable file by stopping the command by using **`Ctrl-C`**.

If the IBM SmartCloud Entry executable file was started with an OSGi console running in the background, you must telnet to it with the correct port to access the console. Refer to OSGi console for more details. From the OSGi console, type `shutdown` to stop IBM SmartCloud Entry and then `exit` to exit immediately. Exit IBM SmartCloud Entry before you restart.

Chapter 9. Uninstalling IBM SmartCloud Entry

The IBM SmartCloud Entry uninstaller, similar to the installer, supports three installation types: console, silent, and swing/graphical installers. Additionally, the uninstaller supports three operating systems: AIX, Linux, and Windows.

For AIX and Linux, the default display type is `console` and the default display type for Windows is `graphical`.

To uninstall IBM SmartCloud Entry using a non-default installation type, start the uninstaller from the command line and enter `-i <uninstall type>` where `<uninstall type>` is `console`, `silent`, or `swing`.

Uninstalling a graphical installation of IBM SmartCloud Entry on Windows

About this task

Use the following steps to uninstall a graphical installation of IBM SmartCloud Entry on Windows:

Procedure

1. Shut down IBM SmartCloud Entry.
2. Access IBM SmartCloud Entry in the Control Panel, **Control Panel** > **Programs** > **Uninstall a program**. Select IBM SmartCloud Entry in the list and then click **Uninstall**.
3. Read the instructions on the Introduction screen. Then, click **Next**.
4. On the Choose Uninstall Features window, select **Uninstall Specific Features** to choose what to uninstall. If you want to completely uninstall IBM SmartCloud Entry, press **Next**. Both Application and Properties product features are cleared.
5. Check the features that you want to uninstall and then press **Uninstall**.

Results

The IBM SmartCloud Entry uninstallation is complete.

Uninstalling a console installation of IBM SmartCloud Entry on Windows

About this task

To uninstall IBM SmartCloud Entry that was installed using a console on Windows, follow these steps:

Procedure

1. Shut down the IBM SmartCloud Entry executable.
2. Open a Windows command prompt.
3. In the command prompt window, navigate to the Windows uninstaller. For example, `cd C:\Program Files\IBM\SmartCloud Entry\_smartcloud_entry_installation`
4. Run the uninstaller by entering `UninstallSCE.exe -i console`
5. Read the uninstaller instructions on the Introduction window and press Enter.

Results

Congratulations, IBM SmartCloud Entry is now uninstalled.

Uninstalling IBM SmartCloud Entry on Linux or AIX

About this task

To uninstall IBM SmartCloud Entry that was installed by using a console on Linux or AIX, follow these steps:

Procedure

1. Stop any IBM SmartCloud Entry processes that are running.
2. Navigate to the uninstaller in the installation folder or in the links folder. For example, `cd /opt/ibm/SCE31/_SmartCloud_Entry_installation`.
3. Run the uninstaller with root authority by running `./UninstallSCE`
4. Read the uninstaller instructions. Then, press **Enter**.
5. In some cases, not all the files cannot be removed by the uninstaller. For example, the links often cannot be removed. To remove the links after the uninstaller completes, follow these steps:
   a. Navigate to the links folder. For example, `cd ~`.
   b. Remove any leftover links with the following command:
   ```
   rm *SCE*
   ```
   c. Repeat this file removal for all remaining files.

Results

The uninstallation is complete.

Uninstalling a graphical installation of IBM SmartCloud Entry on Linux or AIX

About this task

To uninstall IBM SmartCloud Entry that was installed by using a graphical installation on Linux or AIX, follow these steps:

Procedure

1. Stop any IBM SmartCloud Entry processes that are running.
2. Navigate to the uninstaller in the installation folder or in the links folder. For example, `cd /opt/ibm/SCE31/_SmartCloud_Entry_installation`.
3. Run the uninstaller with root authority by running the following command: .
   ```
   ./UninstallSCE -i swing
   ```
4. Read the instructions on the Introduction screen. Press **Next**.
5. On the Choose Uninstall Features window, select **Uninstall Specific Features** to choose what to uninstall. If you want to completely uninstall IBM SmartCloud Entry, press **Next**. Both Application and Properties product features are cleared.
6. In some cases, not all the files cannot be removed by the uninstaller. For example, the links often cannot be removed. To remove the links after the uninstaller completes, follow these steps:
   a. Navigate to the links folder. For example, `cd ~`.
   b. Remove any leftover links by running the following command: `rm *SCE*`
   c. Repeat this file removal for all remaining files.

Results

The IBM SmartCloud Entry uninstallation is complete.

Database cleanup

After IBM SmartCloud Entry is uninstalled, the administrator can optionally drop the database that is associated with IBM SmartCloud Entry. Any database drop and delete commands should be done using the database software.

Chapter 10. Deploying IBM SmartCloud Entry Virtual Appliances for System x

This section describes the procedure for deploying the IBM SmartCloud Entry for System x Virtual appliances. IBM SmartCloud Entry for System x is an integrated cloud management platform that is designed to be quickly deployed and operational. It is installed as a preintegrated software stack and delivered as virtual appliances (also known as vApps).

Note:

- Deploying the IBM SmartCloud Entry virtual appliances for System x is an alternative to using the IBM SmartCloud Entry application installer. For more information about using the IBM SmartCloud Entry application installer, see Chapter 6, "Installing IBM SmartCloud Entry," on page 23.
- IBM SmartCloud Entry for System x version 3.1 supports management of VMware vCenter clusters, KVM hypervisors, and Hyper-V hypervisors.
- KVM appliances are supported by IBM SmartCloud Entry version 2.4 fix pack 2 or higher.
- Hyper-V appliances are supported by IBM SmartCloud Entry version 3.1 or higher.

Prerequisites for IBM SmartCloud Entry Virtual Appliances

Ensure that your virtualization environment meets the minimum requirements for deploying IBM SmartCloud Entry for System x virtual appliances.

Hyper-V appliances

IBM SmartCloud Entry for System x requires an existing installation of Microsoft Hyper-V Server 2012 or Windows Server 2012.

For information about IBM SmartCloud Entry-specific Microsoft Hyper-V installation considerations, see "Microsoft Hyper-V prerequisites" on page 9.

KVM appliances

IBM SmartCloud Entry for System x requires an existing installation of IBM Systems Director Platform Agent and VMControl.

For information about IBM SmartCloud Entry-specific IBM Systems Director and VMControl installation considerations, see "IBM Systems Director VMControl prerequisites" on page 9.

VMware appliance

IBM SmartCloud Entry for System x requires an existing installation of VMware vSphere Enterprise edition that is managed by VMware vCenter Server Standard edition. Ensure that the vCenter Server product is installed, operational, and managing a vSphere environment before you continue with the installation of IBM SmartCloud Entry.

For information about IBM SmartCloud Entry-specific VMware installation considerations, see "VMware prerequisite installation" on page 21

Deploying the Hyper-V virtual appliance

Complete the following instructions to deploy the IBM SmartCloud Entry Hyper-V virtual appliance.

Before you begin

The IBM SmartCloud Entry Hyper-V appliance is shipped as a compressed file on the installation media, along with several other files that are required to deploy the appliance.

To prepare to deploy the Hyper-V appliance, create the following two folders:

- An appliance folder, such as *C:\sceappliance*, that includes the following files from the installation media.
  - IBM_SCE_3.1_x86_HyperV_App.zip - the compressed Hyper-V appliance that is extracted and processed as part of the deployment task. The compressed file contains the following virtual disk files:
    - IBM_SCE_3.1_x86_HyperV_App-disk1.vhdx
    - IBM_SCE_3.1_x86_HyperV_App-disk2.vhdx
    - IBM_SCE_3.1_x86_HyperV_App-disk3.vhdx
    - IBM_SCE_3.1_x86_HyperV_App-disk4.vhdx
  - deploy-SCEAppliance.ps1 - a PowerShell script that is used to deploy the appliance.
  - ovf-env.properties - an editable text file that defines various properties of the new virtual machine. For example, the file defines the virtual machine name, the IBM SmartCloud Entry administrator, and the network configuration.
  - ovf-env.xml.template - a file that is used by the deploy script.
- A virtual machine folder, such as *C:\scevm*, that contains the .vhd files that are attached to the virtual machine when it is deployed. This folder is used as the location for saving snapshots of the virtual machine. The virtual disk files are copied into this folder during the deployment. Files in this folder are required for the new virtual machine to run.

Next, you must customize the virtual machine properties file.

1. Copy the file ovf-env.properties from the source folder to another folder, and then edit the copy. This example copies the file to the virtual machine folder and opens the file for editing.

```
C:\> mkdir \scevm

C:\> copy \sceappliance\ovf-env.properties \scevm\

C:\> notepad \scevm\ovf-env.properties
```

2. Edit the key-value pairs in the ovf-env.properties file to define the configuration of the Hyper-V virtual machine for your environment. A description of each property along with its initial value follows.

   The following properties define the Hyper-V virtual machine configuration values.

   hyper-v.vmname=*SCE_VM*
   The name that Hyper-V uses for the virtual machine.

   hyper-v.vmpath
   The directory where the virtual machine files are located. The virtual disk files are copied here, and a subdirectory is created by Hyper-V to store virtual machine snapshots. The directory must be used only for this virtual machine. Do not delete files in this directory.

   hyper-v.vmmemory=*8GB*
   The memory to be assigned to the virtual machine. A minimum of 8 GB is recommended.

   hyper-v.vmcpu=*4*
   The number of processors to be assigned to the virtual machine. A minimum of four processors is recommended.

   The following properties define IBM SmartCloud Entry configurations values.

com.ibm.skc.admin_id=*admin*
The user name of the initial IBM SmartCloud Entry administrator, used to log in to the IBM SmartCloud Entry user interface.

com.ibm.skc.admin_name=*SmartCloud Entry Administrator*
The display name of the initial IBM SmartCloud Entry administrator, which is displayed in the IBM SmartCloud Entry user interface.

The following properties define the global network configuration values.

netconfig.gateway
The default gateway IP address.

netconfig.dns_server1
The IP address of the primary DNS server.

netconfig.dns_server2
The IP address of the secondary DNS server.

netconfig.domain_name
The DNS domain name of the deployed virtual machine.

netconfig.search_list
An optional DNS search list, which is specified as a comma-separated list of DNS domain names.

netconfig.ntp_server
The IP address of the NTP server that is used to set the virtual machine system clock.

The following properties define the management network configuration. The management network is the private network that is used for communication between the IBM SmartCloud Entry instance and the Hyper-V compute nodes.

hyper-v.eth0.switch
The name of an existing Hyper-V virtual network to be used by the management network interface.

netconfig.eth0.host_name
The system host name to be used for the management network interface.

netconfig.eth0.ip_addr
The IP address to be used for the management network interface.

netconfig.eth0.netmask
The subnet mask to be used for the management network interface.

The following properties describe the customer (public facing) network configuration that is used to access the IBM SmartCloud Entry web interface.

hyper-v.eth1.switch
The name of an existing Hyper-V virtual network to be used by the customer network interface. This switch is required. The virtual machine will have this interface even if you choose not to configure the appliance operating system to use the interface.

netconfig.eth1.second_network=*True*
Configures a second network adapter that can be connected to a customer network when present. If it is not selected, a second network is not configured. The value can be one of the following:

- `True` - The network is configured. If the network uses DHCP, the **netconfig.eth1.use_dhcp** property is required. If DHCP is not used, the **netconfig.eth1.host_name**, **netconfig.eth1.ip_addr**, and **netconfig.eth1.netmask** properties are required.
- `False` - The network is not configured. The **netconfig.eth1.use_dhcp**, **netconfig.eth1.host_name**, **netconfig.eth1.ip_addr**, and **netconfig.eth1.netmask** properties are not used.

netconfig.eth1.use_dhcp

Specifies whether the customer network uses DHCP. The value can be one of the following:

- `True` - DHCP is used. Configuring a second network adapter implies that the customer network has a DHCP server with a host record to ensure a stable IP address within the customer network. If DHCP is used, the **netconfig.eth1.host_name**, **netconfig.eth1.ip_addr**, and **netconfig.eth1.netmask** properties are not used.
- `False` - DHCP is not used. If DHCP is not used, the **netconfig.eth1.host_name**, **netconfig.eth1.ip_addr**, and **netconfig.eth1.netmask** properties are also required.

netconfig.eth1.host_name

The system host name to be used for the customer network interface.

netconfig.eth1.ip_addr

The IP address to be used for the customer network interface.

netconfig.eth1.netmask

The subnet mask to be used for the customer network interface.

The following properties describe the data network configuration. It is used for the managed virtual machines. The data network acts as a trunk interface that allows the quantum agent inside the appliance to get an uplink.

hyper-v.eth2.switch

The name of an existing Hyper-V virtual network. This virtual machine network adapter is configured to use trunk mode.

hyper-v.eth2.nativeVlanID

The VLAN ID to be used to tag packets that are sent by this virtual machine. If packets are not to be tagged, specify `0`. For tagged packets, the VLAN ID must be in the range of `1 to 4094`.

hyper-v.eth2.allowedVlanIDList

The list of VLAN IDs allowed over this trunk. This value can be a combination of individual values and ranges, for example: `hyper-v.eth2.allowedVlanIDList=1, 3, 100-200`

3. Save the customized `ovf-env.properties` file.

About this task

After you define the appliance folder and the virtual machine folder and customized the `ovf-env.properties` file, run the PowerShell script as described in the following steps to deploy the Hyper-V appliance.

Notes:

- The PowerShell script must be run as an administrator. On Windows Server 2012, select the **Run as administrator** action when you open a PowerShell window.
- To run scripts from PowerShell, the execution policy must be set to allow scripts to run. In PowerShell, run the following command for more information:

  ```
  get-help about_execution_policies
  ```
- In addition, the following commands might be helpful:
  - get-executionpolicy
  - set-executionpolicy

Procedure

1. Run the `deploy-SCEAppliance.ps1` script, qualifying the command with the appliance folder name and specifying the location of the `ovf-env.properties` file on the input parameter. For example:

   ```
   PS C:\> C:\sceappliance\deploy-SCEAppliance.ps1 -inputfile \scevm\ovf-env.properties
   ```

In this example, *sceappliance* is the name of the appliance folder and *scevm* is the virtual machine folder.

2. When the script completes, the screen displays the following text:

   ```
   Output logged to C:\scevm\deploy-SCEAppliance.log


   PS C:\>
   ```

   If an error occurs, the output from the command is logged in the `deploy-SCEAppliance.log` in the virtual machine folder. In this example, `C:\scevm\deploy-SCEAppliance.log`.

3. To obtain the latest fixes for the Hyper-V appliance, see "Performing support and maintenance tasks on the IBM SmartCloud Entry for System x appliance" on page 61.

Results

After the Hyper-V appliance is successfully deployed, you can configure the OpenStack cloud in the IBM SmartCloud Entry web interface. For more information, see "Configuring an OpenStack cloud" on page 132.

The following default user names and passwords are shipped with the appliance:

Table 12. IBM SmartCloud Entry default credentials

User name	Password	Description
sysadmin	passw0rd	Used to access the IBM SmartCloud Entry appliance

Table 13. OpenStack credentials

User name	Password	Description
glance	glance	Used for internal communication to glance repository
nova	nova	Used for internal communication to nova controller
cinder	cinder	Used for internal communication to cinder volume management
quantum	quantum	Used for internal communication to quantum networking
gwagent	gwagent	Used for internal communication to the OpenStack Gateway
sceagent	openstack1	Used for communication between IBM SmartCloud Entry and OpenStack
qpidclient	openstack1	Used for communication with QPID messaging server
qpidadmin	openstack1	Used for communication with QPID messaging server
db2inst1	passw0rd	Used for communication between OpenStack and DB2

Additionally, when the appliance is deployed, a new network is configured in Quantum that is called **default**. The default network is the physical network on eth2. Vlans 1 to 4094 are allowed by default.

Deploying the KVM virtual appliance

Follow these instructions to deploy the KVM virtual appliance.

Before you begin

The IBM SmartCloud Entry 3.1 appliance OVA file, `IBM_SCE_3.1_x86_KVM_App.tar`, is shipped as a compressed (TAR) file on the installation media. It must be extracted before deployment. To extract on Linux, use `tar –xf IBM_SCE_3.1_x86_KVM_App.tar`. To extract on Windows, use any compression utility that supports the TAR format.

Procedure

1. In IBM Systems Director, select **Systems Configuration** > **VMControl**.
2. Select the **Virtual appliance** tab and click **Import**.
3. In the Source window, enter the location of OVA (local file system or URL) where the IBM SmartCloud Entry appliance OVA is located and click **Next**.

   Note: This step might take several minutes.
4. If No digital signature was detected for your package, select to **Import without digital signature** and click **Next**.
5. In the Name window, enter a name for the virtual appliance and optionally, enter a description.
6. In the Version Control window, select to **Create a new version tree with the new virtual appliance as the root** and click **Next**.
7. Verify the import summary and click **Finish**.
8. Select to **Run Now** and click **OK**. After the Import process completes successfully, the IBM SmartCloud Entry appliance will be available in the Virtual Appliances list.
9. Select the new Virtual Appliance and click **Deploy Virtual Appliance**.
10. In the Target window, select to **Deploy and create a new virtual server on a host or server system pool** and select the target system. Click **Next**.
11. In the Workload Name window, specify a name for the workload and click **Next**.
12. In the Name window, specify a name for the virtual server and click **Next**.
13. In the Storage Mapping window, select the appliance disks and click **Assign Storage Pool**.
14. Select **Management Storage Pool** and select **OK**.
15. Verify that the Management Storage Pool is selected and click **Next**.
16. In the Network Mapping window, you must map the networks to the actual VLANs or bridges. The OVF contains three source networks that must be mapped:
    - **Management Network**: The private network that is used for communication between the IBM SmartCloud Entry virtual server and the IBM Systems Director server or the FSM.
    - **Customer Network**: The network that connects the managed (provisioned) virtual servers with the general user network. The customer network is intended to be used to make the IBM SmartCloud Entry web user interface accessible for intranet users of the customer.

      Note: Most ports are blocked on this network, except the IBM SmartCloud Entry user interface port.
    - **Data Network**: The data network is used mainly when you are planning to use OpenStack from within the KVM appliance. The data network acts as a trunk interface that allows the Quantum agent inside the appliance to get an uplink. If you are not planning to use OpenStack within the KVM appliance, you can set this network to any bridge or network. The data network is not used in this case.

    Click **Next**.

17. On the IBM SmartCloud Entry Configuration panel, enter or change the following values to customize your IBM SmartCloud Entry installation:
    - **Initial administrator user name**: User name of the initial IBM SmartCloud Entry administrator, used to log in to the IBM SmartCloud Entry user interface.

      Note: The default password is 'passw0rd' and can be changed in the IBM SmartCloud Entry user interface.
    - **Initial administrator name**: Display name of the initial IBM SmartCloud Entry administrator, which is displayed in the IBM SmartCloud Entry user interface. For more information about administrator user name, name, and password, see "Configuring local authentication" on page 80.
18. On the Management Network window, specify the following values to connect the virtual machine to the management network.
    - System host name
    - IP address
    - Subnet mask
19. Optional: On the Customer Network window, enable the network and supply the values.
    - **Use Second Network**: Enables a second network adapter that can be connected to a customer network when present. If it is not selected, a second network is not configured.
    - **Use DHCP**: Configures the second network adapter to use a DHCP server. Configuring a second network adapter implies that the customer network has a DHCP server with a host record to ensure a stable IP address within the customer network. If **Use DHCP** is not set and the **Use Second Network** parameter is selected, then the rest of the fields are required.
    - System host name
    - IP address
    - Subnet mask

    Click **Next**.
20. On the Global Network Settings window, supply the requested values.
    - Gateway
    - Primary DNS
    - Secondary DNS
    - Domain Name
    - DNS suffixes (in order)
    - NTP server

    Click **Next**.
21. Review the summary and click **Finish**. The IBM SmartCloud Entry virtual server will start after deployment finishes. You can right-click on the virtual server and open a Console window to log in to the IBM SmartCloud Entry instance.

Deploying the VMware virtual appliance

IBM SmartCloud Entry is shipped as a VMware virtual appliance that can be deployed to an existing VMware installation.

About this task

Note:

The IBM SmartCloud Entry virtual appliance is configured for access to these networks: a management network, a customer network, and a data network. The management network has access to the VMware vCenter appliance and offers a private DNS server that owns the DNS zones for the private networks.

Often that DNS server is configured to forward DNS queries to customer intranet DNS servers. Optionally, for higher availability, an additional (subordinate) DNS server or servers can be configured in the management network.

At the time of deployment, ensure that the DNS servers that are specified are operational in the management network, serving the zone of the private management network. Do not specify a regular intranet DNS server as primary or secondary DNS server IP because that server is not able to resolve the private IP addresses of the management network.

Virtual machines require a properly configured OS time source to mitigate intrinsic time drift issues. To ensure that the time source is properly configured, all of the pieces of the cloud management stack - virtual machines, hypervisors, switches, and other devices, must be configured to use the same NTP time source. It is common to configure an NTP server on the management server that has access to a time source in the customer intranet or the internet to keep the time. The NTP server can also be the NTP reference in the non-routeable management network

To deploy the virtual appliance, follow these steps:

Procedure

1. Using the VMware vSphere client connect to the VMware vCenter server, select the host on which to deploy the IBM SmartCloud Entry virtual appliance.
2. Click **File** > **Deploy OVF Template.**
3. In the Open window, select `IBM_SCE_3.1_x86_VMware_App.ovf`. Click **Open**.
4. On the Source section of the Deploy OVF Template window, click **Next**.
5. The details of the OVF file are displayed. Click **Next**.
6. Optional: Change the default name. Select the **Inventory Location** for the IBM SmartCloud Entry virtual appliance. Click **Next**.
7. Select the data store or datastore cluster in which to place the IBM SmartCloud Entry virtual appliance. Click **Next**.
8. On the Disk Format window, ensure that **Thick provisioned format** is selected. Click **Next**.
9. Choose the Destination Network for each of the Source Networks. The OVF contains three source networks that must be mapped:
   - **Management Network**: The private network that is used for communication between the IBM SmartCloud Entry instance and the VMware vCenter server.
   - **Customer Network**: The network that connects the managed (provisioned) virtual servers with the general user network. The customer network is intended to be used to make the IBM SmartCloud Entry web user interface accessible for intranet users of the customer.

     Note: Most ports are blocked on this network, except the IBM SmartCloud Entry user interface port.
   - **Data Network**: The data network is used mainly when you are planning to use OpenStack from within the VMware appliance. The data network acts as a trunk interface that allows the Quantum agent inside the appliance to get an uplink. The data network should usually be set to a portgroup with VLAN 4095. If you are not planning to use OpenStack within the VMware appliance, set this network to any network. The data network is not used in this case.

   Click **Next**.
10. On the IBM SmartCloud Entry Configuration panel, enter or change the following values to customize your IBM SmartCloud Entry installation:
    - **Initial administrator user name**: User name of the initial IBM SmartCloud Entry administrator, used to log in to the IBM SmartCloud Entry user interface.

Note: The default password is 'passw0rd' and can be changed in the IBM SmartCloud Entry user interface.

- **Initial administrator name**: Display name of the initial IBM SmartCloud Entry administrator, which is displayed in the IBM SmartCloud Entry user interface. For more information about administrator user name, name, and password, see "Configuring local authentication" on page 80.

11. On the Management Network window, specify the following values to connect the virtual machine to the management network.
    - System host name
    - IP address
    - Subnet mask
12. Optional: On the Customer Network window, enable the network and supply the requested values.
    - **Use Second Network**: Enables a second network adapter that can be connected to a customer network when present. If it is not selected, a second network is not configured. In this case, remove the second network adapter from the IBM SmartCloud Entry vApp property by using the VMware vSphere client
    - **Use DHCP**: Configures the second network adapter by using a DHCP server. Configuring a second network adapter implies that the customer network has a DHCP server with a host record to ensure a stable IP address within the customer network. If **Use DHCP** is not set and the **Use Second Network** parameter is selected, then the rest of the fields are required.
    - System host name
    - IP address
    - Subnet mask

      Note: Consider making the public intranet IP address of the IBM SmartCloud Entry vApp resolve in the customers DNS server to ease the access to IBM SmartCloud Entry.

    Click **Next**.
13. On the Global Network Settings window, supply the requested values.
    - Gateway
    - Primary DNS
    - Secondary DNS
    - Domain Name
    - DNS suffixes (in order)
    - NTP server

    For more information about these values, see Note.

    Click **Next**.
14. Verify the values on the Ready to Complete window and click **Finish**. A progress window displays as the IBM SmartCloud Entry application is deployed.
15. After the deployment finishes, select the created virtual machine. Click **Power On**.
16. From the VMware vSphere Client, navigate to the Console tab.

    Clicking the console gives it focus and causes the mouse pointer to disappear. When you are finished with the console, you can press Ctrl + Alt to release the mouse pointer from the console.
17. Log in to the console by using the following credentials:

    Login: `sysadmin`

    Password: `passw0rd`
18. Run `ifconfig` at the command prompt. Ensure eth0 and eth1 are configured as specified during the OVF deployment.
19. Test communication with the managed server by running `ping -c 4 <Managed Cloud host name>`. If properly connected, all packets should show as received with 0% packet loss:

```
# ping -c 4 192.168.88.9
PING 192.168.88.9 (192.168.88.9) 56(84) bytes of data.
64 bytes from 192.168.88.9: icmp_seq=1 ttl=120 time=1.16 ms
64 bytes from 192.168.88.9: icmp_seq=2 ttl=120 time=0.120 ms
64 bytes from 192.168.88.9: icmp_seq=3 ttl=120 time=0.141 ms
64 bytes from 192.168.88.9: icmp_seq=4 ttl=120 time=0.136 ms
--- 192.168.168.88.9 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3001ms
rtt min/avg/max/mdev - 0.120/0.391/1.161/0.444 ms
```

Managing the IBM SmartCloud Entry appliance

You can configure and manage the IBM SmartCloud Entry appliance for System x by using the SmartCloud Entry Appliance Manager tool (sceappmgr).

About this task

To start sceappmgr, complete the following steps:

Procedure

1. Log in to the IBM SmartCloud Entry appliance virtual machine as `sysadmin`.
2. Run the following command:

   ```
   sceappmgr
   ```

   The following menu displays:

   ```
   IBM-SCE> sceappmgr
   ====================

   Manage SmartCloud Entry Appliance

    1.  Generate Authentication Tokens
    2.  Manage Passwords
    3.  Manage SmartCloud Entry Services
    4.  Manage Volume Groups
    5.  Support and Maintenance

   Enter selection (Enter to cancel):
   ```

   Notes:

   - Pressing **Enter** without making a menu selection exits sceappmgr.
   - The displayed sceappmgr menu reflects the currently available options. For example, menu option 1 might alternatively be Enable OpenStack Services.

Enabling OpenStack services on KVM and VMware

The IBM SmartCloud Entry appliance for System x includes OpenStack services for all of the supported virtualization environments. By default the OpenStack services are disabled on KVM and VMware because OpenStack is used for Hyper-V deployments only. If you plan to use the VMware or KVM appliance to deploy images to a Hyper-V host, you must enable OpenStack services.

About this task

Note: If you enable OpenStack to support Hyper-V deployments, you must also increase the appliance virtual machine resources to four processors and at least 8 GB of memory.

You can enable the OpenStack services by using the SmartCloud Entry Appliance Manager tool (sceappmgr). It configures the required OpenStack services to start when the system is turned on and then starts the OpenStack services. Complete the following steps to enable OpenStack services on a KVM or VMware appliance virtual machine.

Procedure

1. Start the SmartCloud Entry Appliance Manager tool (sceappmgr).
2. Type 1 and press **Enter** to select the option to enable OpenStack. This option is not shown if the OpenStack services are already enabled.
3. Confirm the selection by typing 1 again and pressing **Enter**.

Results

When the OpenStack services are started, the output is displayed, "Done starting OpenStack services."

Generating authentication tokens

You can use the SmartCloud Entry Appliance Manager tool to manage various credentials that are used within the OpenStack services.

About this task

The following credentials can be managed by using the sceappmgr tool.

Keystone SimpleToken

The Keystone SimpleToken is a key that is used for communication between the IBM SmartCloud Entry server and the OpenStack services. After you generate a new SimpleToken, the OpenStack Keystone and IBM SmartCloud Entry servers must be restarted to use the new token.

Admin Token

The Admin Token is a password-like string that can be used with OpenStack commands to authenticate to the Keystone service. It can be used in place of an administrator user ID and password. The OpenStack Keystone server must be restarted before the new Admin Token can be used.

Public Key Infrastructure

Public Key Infrastructure (PKI) keys are used to encrypt the tokens that are passed between the different OpenStack services.

Procedure

1. Start the sceappmgr tool.
2. Select the **Manage Authentication Tokens** option.
3. Select the option for the token that you want to change.

   All of the options require that various portions of the IBM SmartCloud Entry or OpenStack services be stopped briefly.

   The Admin Token can contain only the following US-ASCII characters:

   - a-z, A-Z and 0-9
   - The following special characters: ~`!@#$%^&*()_-+={}[]:;"'<>,.?/

   Leading and trailing spaces are removed.

   When you generate new PKI keys, it is important that the system clock is set correctly before you start. The keys have a valid start date and end date. If the system clock is changed to a time before or after this range, even by a few seconds, the keys will not work until the system time is again within the valid range.

Managing passwords

You can use sceappmgr to manage passwords for IBM SmartCloud Entry, OpenStack, and DB2 on the IBM SmartCloud Entry for System x appliance.

Procedure

1. Start the sceappmgr tool.
2. Select the **Manage Passwords** option.
3. Select the user ID whose password you want to update.
4. You are prompted for the current password, the new password, and a verification of the new password.
5. It might be necessary to restart OpenStack services after you change the password.

Starting, stopping, and status of the IBM SmartCloud Entry application on IBM SmartCloud Entry for System x virtual appliance

You can use the sceappmgr tool to manage the IBM SmartCloud Entry and OpenStack services on the IBM SmartCloud Entry for System x virtual appliance.

With the sceappmgr tool, you can complete the following tasks:

- Start, restart, and stop the IBM SmartCloud Entry application (the IBM SmartCloud Entry service)
- View the status of the IBM SmartCloud Entry application
- Start, restart, and stop the OpenStack services
- View the status of the OpenStack services

To manage services, complete the following steps:

1. Start the sceappmgr tool.
2. Select the **Manage SmartCloud Entry Services** option.
3. Select the operation that you want to complete.

The sceappmgr tool performs the requested operation and displays the output.

Accessing IBM SmartCloud Entry

You can access IBM SmartCloud Entry by opening `http://<IBM SmartCloud Entry host name>:8080/cloud/web/index.html` in a supported browser. To log in for the first time, use the Initial Administrator User Name that you created when you deployed the IBM SmartCloud Entry for System x virtual appliance and the default password, `passw0rd`. It is recommended that you update the password through the IBM SmartCloud Entry web interface.

Note: The port 8080 is the default port. Substitute the correct values for your environment if necessary.

For more information about access, see "Configuring local authentication" on page 80.

Volume group management for the IBM SmartCloud Entry appliance

The IBM SmartCloud Entry appliance for System x provides expandable storage for the OpenStack Glance repository and user data. The SmartCloud Entry Appliance Manager (sceappmgr) provides tools to manage how you allocate storage for these functions.

The OpenStack Glance project provides services for discovering, registering, and retrieving virtual machine images. The IBM SmartCloud Entry appliance for System x is configured to use the file backend, which stores images in the local file system.

Several user data volumes exist that have the potential to grow:

- `/var/log`
- `/home/db2inst1`
- `/home/sysadmin`

- Swap space

The IBM SmartCloud Entry appliance for System x places each of these user data areas on a separate volume. Separating the user data by volume ensures that excessive storage use by one area does not use all of the storage. It also allows more storage to be allocated to each area as needed.

The OpenStack Glance repository and the user data volumes each have a defined Linux Volume Manager (LVM) volume group. The **Image repository** volume group (glance-repository) is used for the OpenStack Glance file backend. The **User data** volume group (user_data_vg) is used for the four user data volumes. Using sceappmgr, you can allocate disks or partitions to these volume groups. For the user data volume group, you can allocate more space to each of the user data volumes. You cannot remove disks, or move storage from one volume group, or volume, to another.

The IBM SmartCloud Entry appliance for System x initially has a 10 GB virtual disk that is allocated to the image repository. The initial size of the image repository is sufficient only for one or two images. It is recommended that you attach a much larger disk to the virtual disk. Further, for future migration, it is recommended that all data on the initial disk be moved to the larger disk and the smaller disk deleted. You can use sceappmgr to manage the disks.

The user data volume group uses a 30 GB virtual disk, which is divided between the four volumes as follows:

- `/home/db2inst1` - OpenStack DB2 database: 10 GB
- `/home/sysadmin` - IBM SmartCloud Entry database, logs, and other files: 10 GB
- Swap space - 5 GB
- `/var/log` - system log files: 5 GB

The IBM SmartCloud Entry appliance for System x supports SCSI and Virtio (on KVM) virtual disks. You can use any storage mechanism that is supported by the hypervisor, such as the following storage devices:

- File-backed virtual disks (for example, vhd and vmdk files)
- Physical disks or partitions that are attached to the hypervisor
- SAN storage
- iSCSI devices

The storage devices must be displayed as block devices to the appliance (with names like `/dev/sda` or `/dev/vda`).

Use the Manage Volume Groups option in the sceappmgr to manage the **Image repository** volume group and the **User data** volume group.

Adding a disk to the image repository volume group (for Hyper-V images only)

To add a disk to the image repository volume group for Hyper-V images, first use the appropriate hypervisor tools to add a new hard disk to the IBM SmartCloud Entry appliance virtual machine. Then, log in to the appliance virtual machine and run the IBM SmartCloud Entry Appliance Manager (sceappmgr) tool.

Before you begin

If the new hard disk that you add was used on another system, ensure that the following requirements are met:

- The disk was not used in a Linux Volume Manager (LVM) volume group by the same name as the volume groups used by the IBM SmartCloud Entry appliance. Ensure that the disk was not in an LVM volume group with the any of the following names:
  - cinder-volumes
  - glance-repository

  - user_data_vg.

  Adding such disks might corrupt the existing LVM volume groups.
- The disk is not recognized by LVM as a physical volume. Such disks are not displayed as available disks when you use the IBM SmartCloud Entry appliance volume management functions. The LVM **pvscan** and **pvremove** commands can be used to detect and correct this situation. Formatting the disk also removes LVM physical volume information.

Note: Importing and exporting LVM volume groups from the appliance to share data is not supported.

Procedure

1. Start the sceappmgr tool.
2. Select the **Manage Volume Groups** option.
3. Select the **Image repository** volume group. The devices that are available to be added to the volume display on the resulting page. The available disk devices include devices that are not mounted as file systems and devices that are not used by the Linux Volume Manager. Disks having only free partitions are also shown.
4. Select a device to add to the volume group. Use the size and disk device information to identify the correct device. The disk device corresponds to the disk controller and location that is available through the hypervisor information for the virtual machine. The device can be an existing partition or an entire disk. If an entire disk is selected, the disk is partitioned to contain a single partition that uses the entire disk. In either case, any existing data on the disk or partition is lost.
5. Enter a selection for whether to add the disk to the volume group, or move the data from the original disk to the new disk. If the appliance is still using the original 10 GB virtual disk, it is recommended that you move the image repository to the new disk.

   Note: The option to move data from the original disk to the new disk is shown only if the original disk is part of the image repository volume group. After the data is moved to the new disk, the original disk is removed from the volume group and this option is no longer shown.

Results

When the appliance virtual machine is restarted, the system formats the disk and adds it to the volume group. The entire volume group is used to host a single logical volume and file system (/mount/glance-repository). Until the system restart is complete, sceappmgr shows the original size for the volume group and indicates that a move or resize is pending. Moving data from the old disk to the new disk can take several minutes, so the system restart is slower than usual.

When the system is restarted, you can use the appropriate hypervisor tools to detach the old disk from the virtual machine. The disk device information that is displayed by sceappmgr can be used to identify the old disk. This information corresponds to the disk controller and location information available from the hypervisor.

Adding disk space to a user data volume

Adding a disk to the user data volume group on the IBM SmartCloud Entry appliance virtual machine is similar to adding a disk to the image repository volume group.

About this task

No file systems are resized when you add a disk to the user data volume group, so you do not need to restart the appliance virtual machine. After you add a disk to the volume group, you can add free space from the volume group to individual volumes.

If you are adding a disk that was used on another system ensure that the following requirements are met:

- The disk was not used in a Linux Volume Manager (LVM) volume group by the same name as the volume groups used by the IBM SmartCloud Entry appliance. Ensure that the disk was not in an LVM volume group with the any of the following names:
  - cinder-volumes
  - glance-repository
  - user_data_vg

  Adding such disks might corrupt the existing LVM volume groups.
- The disk is not recognized by LVM as a physical volume. Such disks are not shown as available disks when you are using the IBM SmartCloud Entry appliance volume management functions. The LVM **`pvscan`** and **`pvremove`** commands can be used to detect and correct this situation. Formatting the disk also removes LVM physical volume information.

Note: Importing and exporting LVM volume groups from the appliance to share data is not supported.

Procedure

1. Start the SmartCloud Entry Appliance Manager (**`sceappmgr`**) tool.
2. Select the **Manage Volume Groups** option.
3. Select the **User data** volume group. A list of the volumes that are part of this volume group are displayed on the resulting page. There is also an option to add a disk to the volume group.
4. Specify the option, Add disk to 'User data' volume group, and press `Enter`. A list of the devices that are available to be added to the volume display on the resulting page. The list of devices includes devices that are not mounted as file systems or used by the Linux Volume Manager. Disks that have only free partitions are also shown.
5. Specify a device to add to the volume group, and press `Enter`. The size and disk device information can be used to identify the correct device. The disk device corresponds to the disk controller and location that is available through the hypervisor information for the virtual machine. The device can be an existing partition or an entire disk. If an entire disk is selected, the disk is partitioned to contain a single partition that uses the entire disk. In either case, any existing data on the disk or partition is lost.
6. The system formats the disk and adds it to the user data volume group. The new size and free space are shown.
7. On the Manage 'User data' Volume Group screen, specify the volume to which you want to add space. Confirm the amount to be added. The system marks the file system to be resized when the system is restarted.
8. After the system is restarted, the file system will reflect the new size.

Performing support and maintenance tasks on the IBM SmartCloud Entry for System x appliance

With the sceappmgr tool you can set the logging level for OpenStack services, collect IBM SmartCloud Entry logs for Support, and migrate from previous versions of IBM SmartCloud Entry. You can also apply fixes and restart or shutdown the IBM SmartCloud Entry for System x appliance.

Procedure

1. Start the sceappmgr tool.
2. Select the **Support and Maintenance** option.
3. Select the operation to be performed.

Results

The sceappmgr tool performs the requested task. A change to the logging level is not implemented until the OpenStack services are restarted. When the system collects logs, a subdirectory with a name like `logs-date` is created in the sysadmin home directory, for example, `logs-2013-04-116_11-37-28`. This directory contains the compressed log or logs.

Example

You can use the Support and Maintenance option to apply fixes and updates for the IBM SmartCloud Entry for System x appliance. Updates and fixes for the component parts that make up the software stack included in the IBM SmartCloud Entry for System x appliance are published in a single fix pack file. After you download the fix pack file to your deployed appliance, selection of a single sceappmgr menu option performs the necessary updates. To download and install updates and fixes for the software stack that is provided by the IBM SmartCloud Entry for System x appliance, complete the following steps:

1. Open your browser to IBM Support Fix Central at http://www-933.ibm.com/support/fixcentral/
2. Click **Select product**.
3. Select **Other Software** for the Product Group.
4. For the Product, select IBM SmartCloud Entry version 3.1.
5. Select **All** for the Installed Version.
6. Select **All** for the Platform and select **Continue**.
7. Identify fixes by selecting **Browse** for fixes and select **Continue**.
8. Select the specific fix that you want and select **Continue**.
9. Authenticate to the Fix Central server to demonstrate entitlement.
10. Select the method that you want to use to download the fix and select **Continue**.
11. Store the appliance fix pack file to a known location on the IBM SmartCloud Entry for System x appliance, such as /tmp.
12. Start the sceappmgr tool (sceappmgr).
13. Select the **Support and Maintenance** option.
14. Select the **Install Fix Pack** option.
15. At the prompt, type the full path and file name of the fix pack file that you downloaded.
16. At the prompt, enter a 1 to start the fix installation process. Stack or operating system services might be stopped and restarted during the installation process. When the process is complete, IBM SmartCloud Entry for System x appliance is updated with the fix pack contents. Progress is reported on the screen and a completion message displays when the updates are completed.

Chapter 11. Installing the IBM SmartCloud Entry Hyper-V Agent

Beginning with version 3.1, IBM SmartCloud Entry can manage Microsoft Hyper-V hypervisors from OpenStack technology. To manage these hypervisors, an IBM SmartCloud Entry Hyper-V Agent must be installed on the Hyper-V endpoint server. This IBM SmartCloud Entry Hyper-V Agent contains packaging of the OpenStack technology that is required to provision to the Hyper-V server. The IBM SmartCloud Entry Hyper-V Agent can be installed on a Microsoft Hyper-V Server 2012 or Microsoft Windows Server 2012 with the Hyper-V role enabled. The IBM SmartCloud Entry Hyper-V Agent must be installed on all managed compute nodes. The IBM SmartCloud Entry Hyper-V Agent installation is packaged as a Microsoft Windows Installer that can be run as an installation wizard, or in silent mode. This installation installs the required OpenStack components on to the Hyper-V server and configures them to run as Microsoft Windows services.

IBM SmartCloud Entry Hyper-V Agent Installation Prerequisites

Use the following steps to prepare your environment for installation.

Preparing Your Hyper-V Server for Installation

On each Hyper-V server that is managed from IBM SmartCloud Entry, a Network Time Service (NTP) must be synchronized with the Hyper-V appliance system that is running the IBM SmartCloud Entry server. See the following document in the OpenStack Compute Administration Guide for more details: Hyper-V Virtualization Platform.

Note: Before you can install the IBM SmartCloud Entry Hyper-V Agent on Microsoft Windows Server 2012 , ensure that the Hyper-V role is enabled on the server.

Supported operating systems

The following operating systems are eligible for IBM SmartCloud Entry Hyper-V Agent installations:

- Microsoft Windows Server 2012 Standard Edition
- Microsoft Windows Server 2012 Datacenter Edition
- Microsoft Hyper-V Server 2012

  Note: Microsoft Hyper-V Server 2012 does not provide the APIs that are needed for IBM SmartCloud Entry to create the ISO image file that provides customization data to virtual machines. To use Microsoft Hyper-V Server 2012 with IBM SmartCloud Entry, you must install a compatible ISO generation utility such as genisoimage from Cygwin.

Note: All Operating Systems must have the latest fix pack applied.

Preparing the Host

The host must be a domain joined computer to support live migration. If the host is not a domain joined computer, you might see the following error display during installation:

```
Failed to modify service settings. Live migrations can be enabled only on a domain joined
computer.
```

Preparing the User

Add the user who installs the Hyper-V Agent for IBM SmartCloud Entry to the Hyper-V Administrators group.

Note: If you are creating the user profile for the first time, the Hyper-V server must be restarted before you install the IBM SmartCloud Entry Hyper-V Agent.

If the user plans to uninstall the Hyper-V Agent in the future, ensure that the user has permission to each of the installation directories on the system.

Installing on Microsoft Windows Server 2012 or Microsoft Hyper-V Server 2012

Follow these steps to install the IBM SmartCloud Entry Hyper-V Agent on Microsoft Windows Server 2012 or Microsoft Hyper-V Server 2012.

Overview of the installation

The installation completes the following steps:

- Create a product installation directory
- Create a Hyper-V external virtual switch (optional)
- Configure Hyper-V Live Migration settings for this host (optional)
- Install an independent Python environment to avoid conflicts with existing applications

  Note: This embedded Python environment is only intended for use by the IBM SmartCloud Entry Hyper-V Agent. Do not attempt to access this environment from any other application. This independent environment is designed to coexist with any preexisting Python environments that might already be installed on the system. Do not install new Python modules into the embedded Python environment.
- Install the required Python modules/packages required by the application
- Install and configure the OpenStack Nova Compute service
- Install and configure the OpenStack Hyper-V Quantum agent for networking
- Register two Windows services, which are set to auto-start by default:
  - **IBM SmartCloud Entry Network Service**
  - **IBM SmartCloud Hyper-V Compute Agent Service**

Important: The 3.1 Hyper-V agent installer does not prevent users from installing a previous version over the more recent Hyper-V agent.

Creating installation or uninstallation logs

Follow these steps to create installation or uninstallation logs for use during the installation or uninstallation of IBM SmartCloud Entry Hyper-V Agent on Microsoft Windows Server 2012.

About this task

Because the IBM SmartCloud Entry Hyper-V Agent installer is MSI-based, you can create an installation or uninstallation log by starting the installer with the `msiexec` command with the correct parameters. Detailed information about creating logs can be found here: How to enable Windows Installer logging.

Installing with graphical Installation

Follow these steps to install the IBM SmartCloud Entry Hyper-V Agent by using the graphical installation wizard.

Procedure

1. For IBM SmartCloud Entry 3.1, download the latest fix for the IBM SmartCloud Entry Hyper-V Agent from Fix Central. For more information, see “Applying fixes and updates for IBM SmartCloud Entry” on page 30.

   Note: The IBM SmartCloud Entry Hyper-V Agent and the IBM SmartCloud Entry Hyper-V appliance must be at the same level, either the GA level, or the fix level.
2. Locate the installation image, and double-click `IBM SmartCloud Entry Hyper-V Agent.msi` to start the installation wizard.
3. Follow the instructions that are provided by the installation wizard. Agree to the license terms, provide an installation destination directory, and select the type of setup you want to use.

   Note: The IBM SmartCloud Entry Hyper-V Agent must be installed to the local C: disk of the server. However, the instance directory (Instances Path) that is used to store virtual machine instance data can be on any local disk.
4. Use the **Nova Compute Configuration** window to configure the compute agent parameters. You can leave the default values provided and manually configure the `nova.conf` file, which is in the `etc\nova` folder, later. The following table shows the mappings between areas from this dialog and properties in the `nova.conf` file.

   Table 14. Nova Compute Configuration fields and related properties in `nova.conf`. Mapping of field names in the installation wizard, related properties in the `nova.conf` file, and installation wizard default values

Area in dialog	Property in **nova.conf**	Installation wizard default values
Glance API Server	*glance_host*	*appliance_mgmt_ip* **Note:** Where *appliance_mgmt_ip* is the IP address of the network interface on the appliance.
Port (after Glance API Server)	*glance_port*	9292
Qpid Server	*qpid_hostname*	*appliance_mgmt_ip* **Note:** Where *appliance_mgmt_ip* is the IP address of the network interface on the appliance.
Port (after Qpid Server)	*qpid_port*	5672
Qpid User Name	*qpid_username*	qpidclient
Qpid Password	*qpid_password*	openstack1
Instances Path	*instances_path*	`C:\Program Files (x86)\IBM\SmartCloud Entry\Hyper-V Agent\instances\`

   Note: The property **`qpid_hostname`** is also written to the file `hyperv_quantum_agent.ini`. For more detailed descriptions about properties in the `nova.conf` file, see the List of configuration options topic in the OpenStack Compute Administration Manual.
5. Use the **Nova Compute Advanced Configuration** window to configure the advanced compute agent parameters. Select **Use Cow Images** to enable the copy on write feature and speed up deployment times. You can also manually configure the `nova.conf` file, which is in the `etc\nova` folder, later. The following table shows the mappings between areas from this dialog and properties in the `nova.conf` file.

Table 15. Nova Compute Advanced Configuration fields and related properties in `nova.conf`. Mapping of field names in installation wizard and related properties in the `nova.conf` file

Area in dialog	Property in **nova.conf**
Use Cow Images	*use_cow_images*
Verbose Logging	*verbose*
Log file	*logdir*

6. Use the **Quantum Network Configuration** window to configure network agent parameters. The installation wizard applies changes that are made to this window to properties in both the `nova.conf` and `quantum.conf` files. You can leave the default values provided and manually configure the `nova.conf` and `quantum.conf` files later. These properties files are in the `etc\nova` and `etc\quantum` folders. The following table shows the mappings between areas from this dialog and properties in the `nova.conf` and `quantum.conf` files.

Table 16. Quantum Network Configuration fields and related properties in `nova.conf` and `quantum.conf`. Mapping of field names in the installation wizard, related properties in the `nova.conf` file and `quantum.conf` file, and installation wizard default values

Area in dialog	Property in **nova.conf** and **quantum.conf**	Installation wizard default values
Quantum Url	*quantum_url*	http://*appliance_mgmt_ip*:9696 **Note:** Where *appliance_mgmt_ip* is the IP address of the network interface on the appliance.
Username	*quantum_admin_username*	quantum
Password	*quantum_admin_password*	quantum
Tenant Name	*quantum_admin_tenant_name*	service
Region name	*quantum_region_name*	*None*
Authentication Url	*quantum_admin_auth_url*	http://*appliance_mgmt_ip*:35357/v2.0 **Note:** Where *appliance_mgmt_ip* is the IP address of the network interface on the appliance.

Note: The file, `hyperv_quantum_agent.ini`, is also updated in the background by the installer. The following properties are updated:

- `rpc_backend=quantum.openstack.common.rpc.impl.qpid`
- `verbose=true`
- `debug=true`
- `control_exchange=quantum`
- `physical_network_vswitch_mappings = *:external`

7. Use the **Hyper-V Live Migration Settings** window to configure the Live Migration settings for the host.

   Note: IBM SmartCloud Entry with Hyper-V supports a Shared nothing live migration. To use live migration, the Hyper-V server must belong a common domain. You can also skip this step and configure the Hyper-V Live Migration setting manually later. See the following document in the OpenStack Compute Administration Guide for more details: Hyper-V Virtualization Platform

   Note: When you provide a user name in the **Nova compute service user** field, ensure that the user you select is a domain user.

8. Use the **Virtual Switch Configuration** window to configure Virtual Switch settings. For more information about Hyper-V Switches, see the following topic:Hyper-V Virtual Switch Overview. If no existing virtual switches are detected, create a new virtual switch. To add a new virtual switch, there must be at least one physical network adapter that is not bound to any existing virtual switch. To manually determine whether a physical network adapter is available, you can use the PowerShell command `get-networkadapter -physical'` to see all physical network adapters. Next, you can use the PowerShell command `get-vmswitch` to see all network adapters that are already in use. A new virtual switch must be exclusively associated with a physical network adapter. No two virtual switches can be associated with the same physical network adapter on the host. See the following document in the OpenStack Compute Administration Guide for more details on using the PowerShell command: Hyper-V Virtualization Platform

   Note: The **Shared for management** property determines whether the Hyper-V Agent can use this physical network adapter to manage network traffic.
9. After you complete the information in the installation wizard, the installation begins.

Installing with silent installation

Because the IBM SmartCloud Entry Hyper-V Agent is installed by using the Microsoft Installer (MSI,), you can start MSI directly without using the graphical installation wizard. This process is called silent (unattended) installation, and is useful for installing this program over a network on a remote system from a shared drive on a LAN server. Follow these steps to silently install IBM SmartCloud Entry Hyper-V Agent on Microsoft Windows Server 2012.

Before you begin

If you choose to install silently, you must create an IBM SmartCloud Entry Hyper-V Agent silent installation response file and use it to drive the installation. The file is addressed in the following sections, and a sample response file is provided for reference

About this task

To install silently, you either provide installation parameters through the command line, or use an INI file (response file) to specify all the parameters in a single file. For both cases, use the `msiexec` command to start the installation. For more information about this command, see Msiexec (command-line options)

Installing silently with the command line

Follow these steps to silently install IBM SmartCloud Entry Hyper-V Agent by using the command line.

Before you begin

If you choose to install silently, you must create an IBM SmartCloud Entry Hyper-V Agent silent installation response file and use it to drive the installation. The file is addressed in the following sections, and a sample response file is provided for reference.

Procedure

1. For IBM SmartCloud Entry 3.1, download the latest fix for the IBM SmartCloud Entry Hyper-V Agent from Fix Central. For more information, see "Applying fixes and updates for IBM SmartCloud Entry" on page 30.

   Note: The IBM SmartCloud Entry Hyper-V Agent and the IBM SmartCloud Entry Hyper-V appliance must be at the same level, either the GA level, or the fix level.
2. To start the installation through the command line directly, open a command prompt and input the following parameters, substituting the IP address and port with your own: `msiexec /i "Hyper-V-OpenStack installer.msi" /qn GLANCE_SERVER="127.0.0.1"  GLANCE_SVR_PORT = "9292"`

Tip: The `/i` parameter means to install, and the `/qn` parameter means that the installation is done with no GUI.

Tip: You can provide as many parameters as you like in the format `key=value`, separated by a space character at the end of the command.

Note: The IBM SmartCloud Entry Hyper-V Agent must be installed to the local C: disk of the server. However, the instance directory (Instances Path) that is used to store virtual machine instance data can be on any local disk.

Example

The following table shows the mappings between parameters in the response file and properties in the `nova.conf` file.

Table 17. Response file parameters and related properties in `nova.conf`. This table shows the mappings between parameters in the response file and properties in the `nova.conf` file.

Parameters in the response file	Property in **nova.conf**
GLANCE_SERVER	glance_host
GLANCE_SVR_PORT	glance_port
QPID_SERVER	qpid_hostname
QPID_SVR_PORT	qpid_port
QPID_UNAME	qpid_username
QPID_PWD	qpid_password
NOVA_INS_PATH	instances_path
COW	use_cow_images
VERBOSE	verbose
NOVA_LOG_PATH	Logdir

The following table shows the mappings between parameters in the response file and properties in both the `nova.conf` and `quantum.conf` files

Table 18. Response file parameters and related properties in `nova.conf` and `quantum.conf` files. This table shows the mappings between parameters in the response file and properties in the `nova.conf` and `quantum.conf` files.

Parameters in the response file	Property in **nova.conf** and **quantum.conf**
QUANTUM_URL	quantum_url
ADMIN_USERNAME	quantum_admin_username
ADMIN_PASSWORD	quantum_admin_password
ADMIN_TENANT_NAME	quantum_admin_tenant_name
REGION_NAME	quantum_region_name
QUANTUM_AUTH_URL	quantum_admin_auth_url
ALLOW_RESIZE_TO_SAME_HOST	allow_resize_to_same_host
QUANTUM_AUTH_STRATEG	quantum_auth_strategy

Note: The property `;AgreeToLicense` in the response file specifies your agreement to the license for the application. Its default value is set to `no`. You must specify `yes` to run the silent installation successfully.

Installing silently with a response file

Follow these steps to run a silent installation by using a response file.

Before you begin

If you choose to install silently, you need to create an IBM SmartCloud Entry Hyper-V Agent silent installation response file and use it to drive the installation. The file is addressed in the following sections, and a sample response file is provided for reference.

Procedure

1. For IBM SmartCloud Entry 3.1, download the latest fix for the IBM SmartCloud Entry Hyper-V Agent from Fix Central. For more information, see “Applying fixes and updates for IBM SmartCloud Entry” on page 30.

   Note: The IBM SmartCloud Entry Hyper-V Agent and the IBM SmartCloud Entry Hyper-V appliance must be at the same level, either the GA level, or the fix level.
2. To run the installation through the response file, you must first enter the correct parameters in your locally saved copy of the response file. See the sample response file that is provided for more details.

   Note: The IBM SmartCloud Entry Hyper-V Agent must be installed to the local C: disk of the server. However, the instance directory (Instances Path) that is used to store virtual machine instance data can be on any local disk.
3. Next, open a command prompt and input the following statement: `msiexec /i "Hyper-V-OpenStack installer.msi" USEINI="reponsefile"`

Example

The sample response file provides an example INI file that can be used to drive a silent installation. This example shows all properties that are available during a graphical installation of the IBM SmartCloud Entry Hyper-V Agent.

```
[Response]
;indicate whether you agree with the liscense and its default value is "no"
;AgreeToLicense=yes
;GLANCE_SERVER = mySCEApplianceHostOrIP
;GLANCE_SVR_PORT = 9292
;QPID_SERVER = mySCEApplianceHostOrIP
;QPID_SVR_PORT = 5672
;QPID_UNAME = qpidclient
;QPID_PWD =
;QUANTUM_URL =
;ADMIN_USERNAME =
;ADMIN_PASSWORD =
;ADMIN_TENANT_NAME =
;REGION_NAME =
;QUANTUM_AUTH_URL =
;QUANTUM_URL_TIMEOUT =
;ALLOW_RESIZE_TO_SAME_HOST =
;QUANTUM_AUTH_STRATEGY =
;INSTANCES1=
;COW = true
;ENABLELOG = 1
;VERBOSE = true
;NOVA_LOG_PATH =
:The path that IBM SCE Hyper-V Agent will be installed.
;INSTALLDIR=


;The string coming after a period is the UUID of the DIM used by the installer internally.
You can actually ignore it during the installation.
```

```
;(IntOpt)Live Migration authentication type you choose. It has two optional values, "0" and "1".
"0" stands for "Kerberos", and "1" stands for "CredSSP".
;LIVEMIGRAUTHTYPE.EDDDE39A_8D99_430B_BFF6_7644F125D2A1 = 0

;NOVACOMPUTESERVICEUSER.EDDDE39A_8D99_430B_BFF6_7644F125D2A1 =

;(IntOpt)The max active virtual machine migrations.
;MAXACTIVEVSMIGR.EDDDE39A_8D99_430B_BFF6_7644F125D2A1 =

;(IntOpt)The max active storage migrations.
;MAXACTIVESTORAGEMIGR.EDDDE39A_8D99_430B_BFF6_7644F125D2A1 =

;(IntOpt)The networks you migrate from. It has two optional values, "0" and "1".
Set "1" means you can migrate from any network, and the following property MIGRNETWORKS will be disabled.
Set "0" means you have to specify the network you migrate from by stating the following property.
;MIGRNETWORKSANY_INTERNAL.EDDDE39A_8D99_430B_BFF6_7644F125D2A1 = 1;

;(IntOpt)Specific network you migrate from. This property only make sense when the
MIGRNETWORKSANY_INTERNAL is set to "0".
;MIGRNETWORKS.EDDDE39A_8D99_430B_BFF6_7644F125D2A1 = 10.10.10.1/32



;(IntOpt) It has two optional values, "0" and "1".Set to "1" means you will skip the virtual switch
configuration,
and the following four properties SKIPNOVACONF, ADDVSWITCH, VSWITCHNAME, VSWITCHNETADAPTER,
NEWVSWITCHNAME, VSWITCHSHARED will be disabled.
Set "0" means you configure the virtual switch during installation.
;SKIPNOVACONF.D5E17CCE_FABA_4230_9715_2DF2AA168F6C = 1

;(IntOpt)Whether to add a virtual switch. It has two optional values, "0" and "1". Set "1" means a new
virtual switch will be add, and the following property  VSWITCHNAME will be disabled.
Set "0" means you will use an existing virtual switch, and the following property VSWITCHNETADAPTER and
NEWVSWITCHNAME will be disabled.
;ADDVSWITCH.D5E17CCE_FABA_4230_9715_2DF2AA168F6C = 0

;(StrOpt)The name of an existing virtual switch you choose.
;VSWITCHNAME.D5E17CCE_FABA_4230_9715_2DF2AA168F6C =

;(StrOpt)The adapter you use to create a new virtual switch.
;VSWITCHNETADAPTER.D5E17CCE_FABA_4230_9715_2DF2AA168F6C =

;(StrOpt)The name you use to create a new virtual switch.
;NEWVSWITCHNAME.D5E17CCE_FABA_4230_9715_2DF2AA168F6C =

;(IntOpt) It has two optional values, "0" and "1".Set to "1" to allow management operating system to
share this network adapter. Set to "0" to disable it
;VSWITCHSHARED.D5E17CCE_FABA_4230_9715_2DF2AA168F6C =

; End of the file
```

Note: The property `;AgreeToLicense` in the response file specifies your agreement to the license for the application. Its default value is set to `no`. You must specify `yes` to run the silent installation successfully.

Note: A response file must start with `[Response]`, followed by any parameters in format `key=value`.

Changing encrypted passwords after installation

Follow these steps to change or decrypt an existing password that is provided during the installation of IBM SmartCloud Entry Hyper-V Agent on Microsoft Windows Server 2012.

About this task

The installation encrypts password-related values such as *qpid_password* and *quantum_admin_password* in both `nova.conf` and `quantum.conf`. You can change or decrypt passwords after installation by using the following information. Ensure that you install the latest fix pack before you complete this task.

Procedure

- To change an encrypted password after installation, use the following command to encrypt a new password string, and then modify the password values in both `nova.conf` and `quantum.conf`.

  ```
  openstack-obfuscate.cmd password
  ```

  where *password* is the new password that you want to encrypt.
- To decrypt an existing encrypted password, use the following command:

  ```
   openstack-obfuscate.cmd -u encrypted password
  ```

  where *encrypted password* is the password that you want to decrypt.

Uninstalling the IBM SmartCloud Entry Hyper-V Agent

The IBM SmartCloud Entry Hyper-V Agent uninstaller supports uninstallation by using the Microsoft Windows Control Panel and command line.

About this task

Use the following steps to uninstall the IBM SmartCloud Entry Hyper-V Agent on Microsoft Windows :

Procedure

1. Shut down the IBM SmartCloud Entry Hyper-V Agent by using the Microsoft Windows Services panel or the appropriate command line.
2. Navigate to Start > Control Panel > Programs > Uninstall a program
3. Select **IBM OpenStack Hyper-V Agent** and click **Uninstall**.
4. Follow the instructions on the uninstallation wizard to complete the operation.

Results

After the IBM SmartCloud Entry Hyper-V Agent is uninstalled, the uninstaller will back up the following files to the `%USERPROFILE%/AppData` folder:

- `nova.conf`
- `quantum.conf`
- `hyperv_quantum_agent.ini`

Note: The uninstaller does not delete any existing instances that you started. These instances are saved in the instances folder.

Uninstalling the IBM SmartCloud Entry Hyper-V Agent on Microsoft Hyper-V Server 2012

The IBM SmartCloud Entry Hyper-V Agent uninstaller supports uninstallation from the Microsoft Hyper-V Server 2012 command line.

About this task

Use the following steps to uninstall The IBM SmartCloud Entry Hyper-V Agent on Microsoft Hyper-V Server 2012 :

Procedure

1. Shut down the IBM SmartCloud Entry Hyper-V Agent by using the Microsoft Windows Services panel or the appropriate command line.
2. 1. Open a command-line window and enter the following command: `WMIC`.
3. Enter the following command to display a list of installed products: `product get name`.
4. Enter the command `product name call uninstall`, where `product name` is the name of the IBM SmartCloud Entry Hyper-V Agent installed product.
5. Enter `Y` to uninstall.

Results

After the IBM SmartCloud Entry Hyper-V Agent is uninstalled, the uninstaller will back up the following files to the `%USERPROFILE%/AppData` folder:

- `nova.conf`
- `quantum.conf`
- `hyperv_quantum_agent.ini`

Note: The uninstaller does not delete any existing instances that you started. These instances are saved in the instances folder.

Enabling nova migration CLI from Hyper-V

IBM SmartCloud Entry 3.1 supports the ability to initiate a live migration of a virtual machine directly from the Hyper-V system by running the OpenStack nova command from the command prompt.

About this task

To enable live migration on Hyper-V, all hosts must run the nova compute service as a Microsoft Windows domain user. The Microsoft Windows domain user must have enough permission to run live migrations. To configure your IBM SmartCloud Entry Hyper-V Agent installation for this support, complete the following instructions on all Hyper-V servers:

Procedure

1. On your Hyper-V host system, navigate to **Control Panel** > **System and Security** > **Administrative Tools** > **Services**.
2. Locate and right-click the **IBM SmartCloud Entry Compute Service**, and select **Properties**.
3. On the **Log On** tab, complete the following steps:
   a. Select the option for **This account**.
   b. Specify the domain user and password to ensure the compute service has appropriate access to the domain resources for a migration.
   c. Click **OK** to save the properties.

Results

To access the nova command, double-click the `AgentConsole.cmd` command from the `bin` directory of your IBM SmartCloud Entry for Hyper-V installation (in the root directory of the installation). A new command prompt opens. Run the **`nova live-migration`** command, following the OpenStack documentation for usage guidance. For more information, see Configuring Shared Nothing Live Migration and Configure and Use Live Migration on Non-clustered Virtual Machines

Note: The AgentConsole that IBM SmartCloud Entry provides on the Hyper-V host can be used only to run the **`nova live-migration`** command. Running other nova or OpenStack commands on the Hyper-V host is not supported.

Enabling Microsoft Hyper-V Server 2012 systems for ISO generation

If you are using Microsoft Hyper-V Server 2012 with IBM SmartCloud Entry, you must install a compatible ISO generation utility such as genisoimage from Cygwin. After you install a compatible ISO generation utility such as genisoimage from Cygwin to use on Microsoft Hyper-V Server 2012 systems, you must update the `nova.conf` file on each system where you installed the IBM SmartCloud Entry Hyper-V Agent.

Procedure

1. Use a text editor to edit the `nova.conf` file that is located at `C:\Program Files (x86)\IBM\SmartCloud Entry\Hyper-V Agent\etc\nova`.
2. Find the line `mkisofs_cmd=C:\Program Files (x86)\IBM\SmartCloud Entry\Hyper-V Agent\bin\ibmgenisoimage.exe` and change the path and file name of the **`mkisofs_cmd`** property to the ISO generation utility that you installed. For example: mkisofs_cmd=C:\cygwin\bin\genisoimage.exe
3. Restart the IBM SmartCloud Entry Hyper-V Compute Agent Service by running the following commands:
   - net stop "IBM SmartCloud Hyper-V Compute Agent Service"
   - net start "IBM SmartCloud Hyper-V Compute Agent Service"

Starting and stopping services

You can start or stop IBM SmartCloud Entry services on the Hyper-V host system from the Microsoft Windows Control Panel.

Procedure

1. On your Hyper-V host system, navigate to **Control Panel** > **System and Security** > **Administrative Tools** > **Services**.
2. Locate the following services:
   - **IBM SmartCloud Entry Network Service**
   - **IBM SmartCloud Hyper-V Compute Agent Service**
3. Right-click on each service and select the appropriate action, either **Start** or **Stop**.

Supporting an additional vSwitch on the Hyper-V compute node

For IBM SmartCloud Entry to support an additional vSwitch, a few manual configuration steps are required.

About this task

The IBM SmartCloud Entry Hyper-V Agent installer assumes that a single Hyper-V external vSwitch is used for all instance data traffic from the compute node. In some cases, a single vSwitch might not be sufficient. Each external vSwitch maps to a single network adapter on the Hyper-V hypervisor. More network adapters and networks might exist that you want to support deployments of instances. To configure an extra vSwitch on the Hyper-V compute node, complete the following steps.

Procedure

1. If you do not already have the vSwitch created, create the additional vSwitch by using the Virtual Switch Manager. The connection type of the new vSwitch must be *external*.

2. Edit the **physical_network_vswitch_mappings** property in the hyperv_quantum_agent.ini file. By default, the file is in the following path: C:\Program Files (x86)\IBM\SmartCloud Entry\Hyper-V Agent\etc\quantum\hyperv_quantum_agent.ini. By default, the property is configured as follows:

   ```
   physical_network_vswitch_mappings=*:vswitch #1
   ```

   Update the property as the following example indicates:

   ```
   physical_network_vswitch_mappings=default:vswitch #1,network2:vswitch #2
   ```

   When a second vSwitch is added to the Hyper-V compute node, the asterisk (*) in the property must be changed to *default* so that it matches the value that is defined on the IBM SmartCloud Entry Hyper-V appliance. If no OpenStack network configuration exists previously, the physical network name, *default*, can be changed to something else. The physical network names that are listed on this property must be configured on the IBM SmartCloud Entry Hyper-V appliance and specified in the IBM SmartCloud Entry web interface when the network configuration is created. Keep the physical network names brief and simple. For example: physnet1, physnet2, public, private, intranet, internet
3. Restart the IBM SmartCloud Entry services on the Hyper-V host system.
   a. On your Hyper-V host system, navigate to **Control Panel** > **System and Security** > **Administrative Tools** > **Services**.
   b. Locate the following services:
      - **IBM SmartCloud Entry Network Service**
      - **IBM SmartCloud Hyper-V Compute Agent Service**
   c. Right-click on each service and select **Restart**.
4. Repeat the previous steps for each Hyper-V compute node. The physical network names, *default* and *network2*, must be the same on each Hyper-V compute node. The vSwitch names can be different on each compute node.
5. On the IBM SmartCloud Entry appliance system, open the console and edit the /etc/quantum/plugin.ini file:

   ```
   sudo vi /etc/quantum/plugin.ini
   ```

   Locate the **network_vlan_ranges** property. By default, the property is configured as follows:

   ```
   network_vlan_ranges=default:1:4094
   ```

   Update the property as the following example indicates:

   ```
   network_vlan_ranges=default:1:4094,network2:1:4094
   ```

   1:4094 specifies the range of VLANs that are assigned for this network if the VLAN ID is not specified in the IBM SmartCloud Entry web interface when an OpenStack network configuration is created. If you want a specific range of VLAN IDs to be used for the network, update the two values as necessary.

   Important: The physical network names that are listed on this property, *default* and *network2*, must match the physical network names that you specified in the hyperv_quantum_agent.ini file earlier in this procedure. Verify that the physical network names are an exact match.
6. Use the SmartCloud Entry Appliance Manager tool to restart the OpenStack services.
   a. Start the sceappmgr tool.
   b. Select the **Manage SmartCloud Entry Services** option
   c. Select the option to **Restart OpenStack services**.
7. After OpenStack is restarted, use theIBM SmartCloud Entry web interface to create a new OpenStack network configuration. At the bottom of the network configuration page, specify *network2* for the physical network name. The network type must be either **Flat** or **VLAN**.

8. Deploy an image by using the new network configuration. The network adapter of the deployed instance is assigned to the vSwitch that you specified in the `hyperv_quantum_agent.ini` file earlier in this procedure.

Chapter 12. Configuring IBM SmartCloud Entry home directory properties

After successfully installing IBM SmartCloud Entry, there is a directory that is called `/.SCE31`. This directory is the IBM SmartCloud Entry home directory and contains all of the IBM SmartCloud Entry configuration property files and log files.

The `/.SCE31` directory is created at the following default locations, which are based on platform:

- On Windows platforms, the default location is the user home directory.
- On Linux or AIX platforms, the default location is the `/var/opt/ibm` directory.

The `authentication.properties` settings are required for IBM SmartCloud Entry to interface with your cloud manager. The other features provide flexibility and convenience.

You can configure some IBM SmartCloud Entry features through the IBM SmartCloud Entry web user interface, but all IBM SmartCloud Entry features are configurable through the configuration files that are found in the IBM SmartCloud Entry home directory.

To configure basic properties and features of IBM SmartCloud Entry, you must modify properties that are defined within the configuration files in the home directory. These configuration files include the following:

authentication.properties
Specifies the user authentication type to use for IBM SmartCloud Entry.

database.properties
Specifies the database type and path.

email.properties
Specifies email notification capabilities.

cloud.properties
Specifies the common configuration of IBM SmartCloud Entry and the URL for the User Guide documentation.

deployment.properties
Specifies properties for configurations of virtual appliances to simplify deployments for cloud users.

logging.properties
Specifies IBM SmartCloud Entry log file properties.

networkConfiguration.properties
Specifies network configurations for deployments.

billing.properties
Enables charging for cloud resources upon deployment.

metering.properties
Enables metering for cloud resources upon deployment.

web.properties
Specifies properties for the user interface configuration.

server.properties
Specifies properties for enabling the optional Secure Sockets Layer (SSL) configuration.

Notes:

- If you do not know your user home directory in a Windows OS, enter `%HOMEPATH%` in the address bar of a Windows Explorer window.
- If you modify these properties while the IBM SmartCloud Entry server is active, you must stop and restart IBM SmartCloud Entry for the new property values to take effect.

Configuring user registry authentication

IBM SmartCloud Entry supports two types of authentication mechanisms: Lightweight Directory Access Protocol (LDAP) and Local, where authentication is performed by using the IBM SmartCloud Entry local user registry.

LDAP provides the highest level of security for production environments. Local authentication is intended only for non-production environments, such as for a proof of concept or for performing a demonstration.

The web interface is the primary way to configure LDAP, but the `ldap.xml` file can also be edited when necessary.

LDAP authentication

The IBM SmartCloud Entry includes an LDAP authenticator that is designed to authenticate users in a wide range of environments, whether the authentication process is a simple bind or a multistage process.

LDAP authentication is performed by defining a series of steps for the authentication process, defining the inputs and outputs of each step, and then running them in sequence. If all the steps run successfully, the user is authenticated.

Configuring LDAP authentication manually

Beginning in IBM SmartCloud Entry 3.1 the web interface is the primary means of configuring LDAP. If you have a migrated LDAP configuration from a previous release, or if you want to enable user name case sensitivity, you can edit the `ldap.xml` configuration file.

For more information about configuring LDAP by using the web interface, see “Configuring LDAP authentication using the web interface” on page 115.

Properties of an LDAP authentication step

Host A string host name for the LDAP host. This property is required.

Search Context
If an LDAP lookup is to be performed, a search context must be provided. This property is required only if a search filter is provided.

Search Filter
If an LDAP lookup is to be performed, a search filter format string must be provided. This string tells the authenticator how to create a search filter that ensures that only one result is returned, as LDAP does not guarantee ordering of results if there are more than one. Additionally, the string *FILTER* is a special value in the search filter. This string is replaced with the user ID entered during login. If you do not use the string *FILTER* in your configuration file, there is no replacement during authentication. If the strings that are defined in your configuration file are static, and a search context is provided, the search filter property is required.

Authentication DN

This property specifies the distinguished name (DN) used for authenticating to the LDAP server. If you are using this property to perform a search, you can specify the property as:

```
</authDN password="password">dnname</authDN>
```

If the property is specifying the DN to use for authentication, define the DN in one of the following ways:

- The DN can be constructed from the user ID. For example, the DN for a user logging in as *joe* can be constructed by using the following:

  ```
  <authDN>uid={FILTER},ou=people,dc=site</authDN>
  ```

  This example creates the DN `uid=joe,cn=users,ou=people,dc=site`
- The DN of the LDAP user entry that is returned by a previous search step is represented using the special value {PERSON_DN}, as shown in this example:

  ```
  <authDN>{PERSON_DN}</authDN>
  ```

In both cases, the password that the user entered to log in is also used to authenticate to the LDAP server.

To perform an anonymous search, do not specify the authentication DN property.

Admin Users

This attribute specifies a list of LDAP user accounts to be given administrator privileges:

```
<adminUsers>admin@company.com,me@company.com</adminUsers>
```

User name case sensitive

This attribute specifies whether the LDAP server defines the user name as case sensitive or not.

```
<userNameCaseSensitive>true</userNameCaseSensitive>
```

Secure connection enablement

This attribute specifies whether to enable a secure connection for LDAP authentication. Some LDAP servers enable the **StartTLS** operation by default, and other LDAP server do not. As an administrator, you can turn off the secure connection, if the LDAP server does not support **StartTLS** operation. The possible values for this attribute are **`true`** or **`false`**. To enable a secure connection, specify this property in the config element:

```
<enableSecureConn>true</enableSecureConn>
```

Outputs

This value indicates what information is needed during the current step for the next step and how to pass that information along. The Outputs value is essentially a list of instructions that gets an attribute value, for example *foo*, and passes it along as *bar*. This value is optional.

- **User account name**: An output can be flagged as the name for a user account by adding `attribute="fullname"` to the output tag. This value is retrieved and used as the user name by IBM SmartCloud Entry. If you do not specify this value, the user ID is used for the user display name.
- **User e-mail address**: An output can be flagged as the email for a user account by adding `attribute="email"` to the output tag. This value is retrieved and used as the user email address by IBM SmartCloud Entry.

Example of an ldap.xml file

In this example of an `ldap.xml` file, an authenticated secure search is performed to find the directory entry where the mail attribute matches the value that is passed into the username field.

```
<?xml version="1.0"?>
<config>
 <host>ldap://ldap.company.com</host>
  <adminUsers>admin@company.com,me@company.com</adminUsers>
  <enableSecureConn>false</enableSecureConn>
  <userNameCaseSensitive>true</userNameCaseSensitive>
  <step>
      <authDN password="password">cn=ldapAdmin,ou=directory,o=company.com</authDN>
      <searchFilter>(|(mail={FILTER}))</searchFilter>
      <searchContext>ou=directory,o=company.com</searchContext>
      <outputs>
```

```
         <output attribute="fullname">
            <get>cn</get>
         </output>
      </outputs>
    </step>
    <step>
        <authDN>{PERSON_DN}</authDN>
    </step>
</config>
```

Changing authentication mode

You can change the IBM SmartCloud Entry to LDAP authentication mode by editing the `authentication.properties` file.

About this task

Note: Beginning in IBM SmartCloud Entry 3.1, the web interface is the primary means of configuring LDAP. If you use the web interface to configure LDAP, the steps in this task are not required. For more information about configuring LDAP by using the web interface, see "Configuring LDAP authentication using the web interface" on page 115.

To change IBM SmartCloud Entry to LDAP authentication mode, complete the following steps:

Procedure

1. Open the `authentication.properties` file in the home directory.
2. Set the `authentication.type` property to *LDAP* as shown in the following example:
   ```
   authentication.type=LDAP
   ```
3. Open the `ldap.xml` file in the home directory.
4. Configure the LDAP steps as described in the "Configuring LDAP authentication manually" on page 78.
5. Restart the IBM SmartCloud Entry server.

   You can change the authentication mode back to local by setting the `authentication.type` property back to *LOCAL*.

Configuring local authentication

By default IBM SmartCloud Entry is set up to use local authentication mode. Local authentication is intended only for non-production environments such as for a proof of concept or for performing a demonstration. For production environments, configure LDAP to ensure the highest level of security.

About this task

Validate the configuration by following these steps:

Procedure

1. Open the `authentication.properties` file in the home directory.
2. Configure the `authentication.type` property to use local authentication, such as:
   ```
   authentication.type=Local
   ```
3. Configure the default administrator user name, name, and password, such as:
   ```
   admin.username=admin
   admin.name=SCE Administrator
   admin.password=<password>
   ```

   Note: These fields might already be populated or configured during installation. The values of the administrator user name, name, and password that are used here are examples. You must update these values according to business or security guidelines. There is a limitation that prevents too many invalid login attempts. A user can try three login attempts to IBM SmartCloud Entry within a 24 hour period. The users, both the user and administrator roles, are locked out if three login requests fail. However, the administrator is able to unlock them. To configure this limitation, enable the following property: *com.ibm.cfs.failedlogincheck.enabled=false*. This property is disabled by default.

Configuring REST API authentication

You can configure IBM SmartCloud Entry to require authentication when it calls to the IBM SmartCloud Entry REST APIs.

About this task

IBM SmartCloud Entry supports the following authentication methods:

- Basic HTTP authentication for a user login and REST API-based validation
- Encrypted token-based authentication for REST API calls

The basic strategy for using encrypted tokens is as follows:

- HTTP/REST agents (browser or REST client) initially use the login authentication REST API to authenticate their user ID and password credentials.
- The user ID and password are validated against the LOCAL or LDAP repository (depending if LOCAL or LDAP is configured).
- Upon successful login authentication, an encrypted token and its expiration are returned in the login response.
- The agent can use (as an HTTP header cookie) the encrypted token for subsequent REST API calls to identity themselves until the token expires.
- After the authentication token expires, the agent must use the login REST API again to validate their user ID and password. When complete, the agent obtains a new authentication token.

Note: The system that is running the IBM SmartCloud Entry web interface or REST client must have the date, time, and time zone that is correctly configured for its physical location.

To require authentication when IBM SmartCloud Entry calls to the Rest APIs, complete the following configuration steps:

Procedure

1. Open the `authentication.properties` file in the home directory.
2. Set the authentication.secure property to `true` as shown in the following example:

   ```
   authentication.secure=true
   ```

   When the property is set to `true`, the caller is prompted for credentials before it processes the API request. The credentials are validated against the user registry that is configured, such as Local or LDAP.
3. If IBM SmartCloud Entry is configured to use Single Sign On with other SmartCloud products, you must set the shared secret key. Use the same shared secret key in all applications by using Single Sign On. If IBM SmartCloud Entry is not using Single Sign On, leave the property unset and the application generates and save a new secret key when it first starts.

   ```
   com.ibm.cfs.token.key=The Secret Encryption Key
   ```
4. Optional: Set the name of the HTTP header cookie. The cookie is used to transport the encrypted authentication token. This property specifies the name of the HTTP header cookie, which is used in HTTP REST API requests to transport the encrypted authentication token. The default value is *simpletoken*.

   ```
   com.ibm.cfs.token.header.field.name=simpletoken
   ```

5. Optional: Set the time duration for authentication tokens (in seconds). This time duration determines how long an authentication token is valid. After a token expires, the agent must obtain a new token by using the login authentication REST API.

   ```
   com.ibm.cfs.token.duration=14400
   ```
6. Optional: Disable automatic renewal for the authentication token. When enabled, authentication tokens renew (by using the specified duration period) each time they are successfully used on an API call. If this option is disabled, the only way to renew an authentication token is to obtain a new token by using the login authentication REST API.

   ```
   com.ibm.cfs.token.autorenew.enabled=false
   ```
7. Restart your IBM SmartCloud Entry server for the changes to take effect.

Configuring database

By default, IBM SmartCloud Entry uses an internal Derby database which is created inside the home directory. For larger environments, you might want to use an external database. IBM SmartCloud Entry supports using an external DB2 database.

About this task

For more information about installing DB2, see “Database prerequisites (optional)” on page 22.

IBM SmartCloud Entry also supports initial use of a Derby database and migration to a DB2 database at a future point. For details on the migration process, see “Migrating a Derby database to DB2 database” on page 38.

To change the IBM SmartCloud Entry database configuration to use DB2, complete the following steps:

Procedure

1. Open the `database.properties` file in the home directory.
2. Set the database.type property to DB2, as shown in the following example:

   ```
   database.type=db2
   ```
3. Set the database.username property to the user ID defined for the database, as shown in the following example:

   ```
   database.username=<db2user>
   ```
4. Set the database.password property to the password ID defined for the database, as shown in the following example:

   ```
   database.password=<db2passwd>
   ```

   Note: The clear text password is replaced with an encrypted password after IBM SmartCloud Entry launches the first time.
5. Set the database.db2.path property to the location of the DB2 database, as shown in the following example:

   ```
   database.db2.path=//localhost:50000/cfs:
   ```

   Note:

   - One or more connection directives can be appended to the database path, and they must be separated by a semicolon. For example:

     ```
     database.db2.path=//localhost:50000/cfs:retrieveMessagesFromServerOnGetMessage=true;
     ```
   - Replace `localhost` with a full IP address (it can be a remote host) and verify the port number. Here are a few links to help you find the port number:

UNIX: http://publib.boulder.ibm.com/infocenter/cmgmt/v8r3m0/index.jsp?topic=%2Fcom.ibm.sysadmin.hlp%2Fcsa10010.htm or as a potential shortcut, use the `grep i db2 /etc/services` command.

Windows: http://publib.boulder.ibm.com/infocenter/cmgmt/v8r3m0/index.jsp?topic=%2Fcom.ibm.sysadmin.hlp%2Fcsa10010.htm or as a potential shortcut, look for the DB2 entries in the services file at `C:\WINDOWS\system32\drivers\etc\services`.

Configuring email notifications

IBM SmartCloud Entry sends email notifications for several relevant user and administrator events such as an instance completion, instance failure, new user account requests, and new user accounts created. In order to take advantage of these notification capabilities, you must configure the notification properties in the home directory.

About this task

To set up notification for IBM SmartCloud Entry follow these steps:

Procedure

1. Open the `email.properties` file in the home directory.
2. Set the `com.ibm.cfs.email.relay.host` property to the host name of the relay host that IBM SmartCloud Entry uses for outgoing SMTP emails.
3. Optionally, you can set the email subject prefix for all IBM SmartCloud Entry emails and the "from" name, by setting the following properties:
   ```
   com.ibm.cfs.email.subject.prefix
   com.ibm.cfs.email.from.name
   com.ibm.cfs.email.from.address
   ```
4. Save the `email.properties` file and restart the IBM SmartCloud Entry server.

   You can globally disable email notifications in IBM SmartCloud Entry by setting the `com.ibm.cfs.email.default.notifications` property in the `email.properties` file to `false`.

   Individual users can disable notifications through the IBM SmartCloud Entry web user interface.

   Note: Ensure that the IBM SmartCloud Entry administrator has an email address that is configured to receive notifications.

Configuring common cloud properties

Common cloud properties are configured by providing information such as the refresh interval and online help configuration in the `cloud.properties` file.

About this task

To configure your cloud manager, do the following:

Procedure

1. Open the `cloud.properties` file in the home directory.
2. Edit the properties by providing values for each configuration property.
3. Save the `cloud.properties` file and restart the IBM SmartCloud Entry server.

Cloud refresh interval

IBM SmartCloud Entry checks for new images and instances in the cloud and synchronizes the properties for these images and instances.

By default, IBM SmartCloud Entry receives messages from the cloud to synchronize with the cloud manager. The frequency of this synchronization is determined by the `com.ibm.cfs.cloud.refresh.interval` property in the `cloud.properties` file. If the property is not set, a default of 30 seconds is used.

IBM SmartCloud Entry scans the cloud for updates on instances as often as the refresh interval property specifies. However, you can change the synchronization mode so that IBM SmartCloud Entry periodically checks with the cloud without waiting for messages.

For more information about setting the synchronization mode, see “Configuring cloud synchronization mode” on page 86.

Cloud online help configuration

The IBM SmartCloud Entry has a configurable documentation property that enables IBM SmartCloud Entry to open the User Guide when the Help link is selected by the user.

About this task

To configure the URL for the Help documentation, follow these steps:

Procedure

1. Open the `cloud.properties` file in the home directory.
2. Configure the property `com.ibm.cfs.cloud.documentation` to be set to the URL for the User Guide location. By default, this property is set to the IBM SmartCloud Entry User Guide. Using the default property setting, the user can access the User Guide on the IBM SmartCloud Entry wiki in any of the supported languages by selecting the link for the language of choice. If something other than this default behavior is wanted, the property can be changed to any URL where the User Guide document is located.

Configuring global image deployment

Image deployment customization properties that apply equally to all images in the IBM SmartCloud Entry image library can be configured through the `deployment.properties` configuration file in the home directory.

To simplify the image deployment process for IBM SmartCloud Entry users, configure all of the images before you make IBM SmartCloud Entry available to users. Image property customization often requires knowing the low-level details of the environment or having advanced knowledge of the data center.

You can configure image deployment customization properties through the IBM SmartCloud Entry web user interface for individual image settings or through the `deployment.properties` file in the home directory for global image settings. For more information about configuring individual image settings, see “Configuring image deployment properties” on page 119.

The contents of the `deployment.properties` configuration file depend on what is expected by the cloud manager software, either VMware, VMControl, or OpenStack and what hardware is available.

Note: Global configurations are refreshed only when manually reset or when the deployment target changes.

VMControl

For VMControl, these properties correspond to Open Virtualization Format (OVF) properties that are found in the images that are used by the manager software. Any customization property that is expected by the cloud manager can be specified here as a default global property for all subsequent deployments.

For VMControl image customization information, see the customization APIs found in the IBM Systems Director VMControl SDK, such as the virtualAppliances/{virtualApplianceOID}/customization API.

VMware

When you use VMware as the cloud manager, the following properties are supported for Linux and Windows images:

```
vmware.linux.dns1=9.8.8.8
vmware.linux.dns2=9.8.8.7
vmware.linux.hostname=myhost
vmware.linux.domainname=cloud.company.com

vmware.windows.computername=WINDOWS
vmware.windows.workgroup=WORKGROUP
vmware.windows.timezone=20
vmware.windows.username=John Doe
vmware.windows.organization=Cloud Company
vmware.windows.productkey=xxxx-xxxx-xxxx-xxxx-xxxx
vmware.windows.password=Default_password_for_windows_deployments

vmware.dnssuffixlist=cloud.company.com,company.com

vmware.networkdevice.Network adapter 1.network=VM Network
vmware.networkdevice.Network adapter 1.usedhcp=false
vmware.networkdevice.Network adapter 1.ipaddress=
vmware.networkdevice.Network adapter 1.netmask=255.255.255.0
vmware.networkdevice.Network adapter 1.gateway1=9.9.9.9
vmware.networkdevice.Network adapter 1.gateway2=
vmware.networkdevice.Network adapter 1.dns1=9.8.8.8
vmware.networkdevice.Network adapter 1.dns2=9.8.8.7
vmware.networkdevice.Network adapter 1.primaryWINS=9.8.8.10
vmware.networkdevice.Network adapter 1.secondaryWINS=9.8.8.11
```

For VMware, you can also find these properties in the `deployment.properties` file.

OpenStack

When you use OpenStack as the cloud manager, the following properties are supported for Linux and Windows images in the `deployment.properties` file:

```
openstack.openstack.flavors
openstack.openstack.keypairs
openstack.openstack.server.personality.source.[1-5]
openstack.openstack.server.personality.target.[1-5]
openstack.openstack.server.customizations
openstack.networkdevice.Network adapters.networks
```

More deployment properties are available for images that have a configuration strategy. For more information about configuration strategies, see “Configuring images with OpenStack” on page 96.

Configuring a deployment target

By default, IBM SmartCloud Entry deploys images to any known pool or host in the cloud, where "pool" refers to a system pool when you are using VMControl or a resource pool when you are using VMware. OpenStack only supports the cloud as the deployment target. For VMControl and VMware, you can set a different default global deployment target.

About this task

To change this default target selection strategy, follow these steps:

Procedure

1. Open the `deployment.properties` file in the home directory.
2. Set the value of the `com.ibm.cfs.deployments.target.strategy` property to any of the following target selection strategies:

   byName
   Use the target with the given name. The name might refer to a host, system pool, resource pool, or cluster depending on the type of cloud adapter that is being used. Set the property value to `byName:{targetName}`, where `{targetName}` is the actual name of the desired system.

   byID
   Use the system with the specified ID. For VMControl, this ID is the OID of the target system pool or host. Set the property value to `byID:{targetOID}`, where `{targetOID}` is the actual OID of the desired system.

   anyPool
   Use any system that is a pool.

   anyHost
   Use any system that is a physical host.

   anyPoolOrHost
   Use any pool or physical host.

   anyCluster
   Use any cluster (applicable to VMware only).

   anyTarget
   Use any pool or host for VMControl and use any pool or host or cluster for VMware.
3. Save the `deployment.properties` file and restart the IBM SmartCloud Entry server.

Configuring cloud synchronization mode

IBM SmartCloud Entry scans the cloud for updates on instances as often as the refresh interval property specifies. However, you can change the synchronization mode so that IBM SmartCloud Entry periodically checks with the cloud without waiting for messages.

To change the sync mode, open the `deployment.properties` file and modify the following settings:

```
com.ibm.cfs.cloud.sync=push
```

To enable IBM SmartCloud Entry to synchronize with the cloud by using periodic checking, set this property to `poll`. Enable the configuration by ensuring that you uncomment the **`com.ibm.cfs.cloud.sync`** line (remove any preceding # symbol).

For more information about setting the refresh interval, see “Cloud refresh interval” on page 83.

Configuring a staging project

By default, IBM SmartCloud Entry scans the cloud for new images periodically. When IBM SmartCloud Entry finds a new image or instance, it places it in the Public project where all users have access to it. However, you can configure a staging project to store newly discovered images or instances, allowing administrators to configure images before making them available to other users.

For more information about newly discovered images, see Cloud refresh interval.

To configure this staging project, add or uncomment this line in the `deployment.properties` file:

```
com.ibm.cfs.staging.project=Staging
```

Save the `deployment.properties` file and restart the IBM SmartCloud Entry server. The property takes effect after the server is restarted.

Note: When using the VMware adapter, virtual servers that are defined as templates on the vCenter server are automatically discovered and displayed on the IBM SmartCloud Entry Images area. The IBM SmartCloud Entry administrator defines which images belong to which user profiles and therefore defines which VMware virtual server templates a user can access. IBM SmartCloud Entry discovers all virtual server templates regardless of which datacenter they reside in. There is currently no option to limit IBM SmartCloud Entry to specific datacenters.

Configuring global priority of an instance when relocating

IBM SmartCloud Entry enables you to choose whether you want your users to update the global priority of an instance when relocating the instance from host to host. *Instance priority* is the priority for relocating instances from one host to another host, when the instance is deployed in a pool. Depending on your site administration policies, you might not want users to change the priority of instances.

About this task

To configure the ability of updating instance priority, follow these steps:

Procedure

1. Open the `deployment.properties` file in the home directory.
2. To disable the ability to update instance priority, set the `com.ibm.cfs.deployments.update.priority` property to *false*. The default value of this property is *false*. If this property does not exist in the `deployment.properties` file, add it to the file.
3. Save the `deployment.properties` file and restart the IBM SmartCloud Entry server.

Configuring access to advanced deployment form

IBM SmartCloud Entry allows you to choose whether you want your users to see the advanced deployment form or just the basic deployment form.

About this task

The advanced deployment form allows a user or administrator to access all of the image properties that can be configured when an image is deployed. The basic deployment form contains only a subset of the image properties. Depending on your site administration policies, you may or may not want to show this advanced panel to the user.

To configure the visibility of the advanced deployment form, follow these steps:

Procedure

1. Open the `deployment.properties` file in the home directory.
2. Set the `deployment.advanced.form.enabled` property to *true*. This value enables the advanced deployment form so that it is displayed to all users. The default value of this property is *false*; users, by default, do not see the advanced deployment form.
3. Save the `deployment.properties` file and restart the IBM SmartCloud Entry server.

Results

Note: Administrators can also configure which advanced properties are shown on the basic deployment form. Use the web interface to configure those values for an image. When the `deployment.advanced.form.enabled` property is set to *true*, project owners can also configure which advanced properties are shown on the basic deployment form

Configuring the number and maximum size of additional storage

IBM SmartCloud Entry interface allows a user to add additional secondary disks to a virtual image using the Add Storage property. Adding additional secondary disks is also supported for VMware when you are deploying an image. IBM SmartCloud Entry provides a configurable property to set the maximum number of disks that can be attached to a virtual machine. This property applies during and after deployment of the virtual machine.

About this task

Note: This feature is not supported if the following statements are true:

- The virtual machine is deployed in the Shared Storage Pool.
- The instance that is being deployed is an IBM i instance.

To configure the secondary disk properties, follow these steps:

Procedure

1. Open the `deployment.properties` file in the home directory.
   - To set the maximum number of disks to use, edit the `com.ibm.cfs.vs.max.disks` property. The default value of this property is `3`.
   - To set the maximum size in megabytes, edit the `com.ibm.cfs.vs.max.disksize` property. The default value of this property is `2048000`.
2. Save the `deployment.properties` file and restart the IBM SmartCloud Entry server.

Configuring Storage Copy Services (SCS) capture repositories (VMControl only)

IBM SmartCloud Entry allows you to specify that you want all captured workloads to be saved in the Storage Copy Services (SCS) repository

Before you begin

In order to configure this option, you must know the object ID (OID) of the VMControl image repository. To find this OID, run the IBM Systems Director CLI command **`smcli lsrepos -o`** as shown in the following example, where the SCS repository is 6838. The results also show a second repository with an OID of 3795, but note that is not the SCS repository and so it can be ignored for the purposes of this configuration example.

```
smcli lsrepos -o
DEV2_V7K_Image_Repository, 6838
icb-mgr, 3795
```

About this task

This configuration is optional and only needed if you have multiple image repositories in your environment, and you want to select one repository over another. By default when a user captures a workload, the first SCS repository found is used. To configure a different SCS capture repository to be used, follow these steps.

Procedure

1. Open the `deployment.properties` file in the home directory.
2. Set the `com.ibm.cfs.vmc.capture.repository.scs` property to the VMControl OID of the repository.
3. Save the `deployment.properties` file and restart the IBM SmartCloud Entry server.

Configuring retry for a failed deploy or delete action (VMControl only)

IBM SmartCloud Entry can retry failed VMControl deployments and deletions one time.

About this task

To enable the automatic retry, follow these steps:

Procedure

1. Open the `deployment.properties` file in the home directory.
2. Set the `com.ibm.cfs.vmc.deployment.retry.reasons` to `.*`

   ```
   # A command-separated list of error codes from VMControl or Director for which
   # a deployment should be re-attempted, because it may succeed the second time.
   # This is an advanced setting and should not be modified unless really necessary.
   # Use .* to retry for any reason
   com.ibm.cfs.vmc.deployment.retry.reasons=.*
   ```
3. Set the `com.ibm.cfs.vmc.deployment.deletion.retry.reasons` to `.*`

   ```
   # A command-separated list of error codes from VMControl or Director for which
   # a deployment deletion should be re-attempted, because it may succeed the second time.

   # This is an advanced setting and should not be modified unless really necessary.
   # Use .* to retry for any reason
   com.ibm.cfs.vmc.deployment.deletion.retry.reasons=.*
   ```
4. Set the `com.ibm.cfs.vmc.deployment.deletion.retry.timeout` to 5

   ```
   # The timeout in minutes for the thread that waits for the VMControl workload to stop
   # before we attempt to delete it again . This is a VMControl workaround. Default is 5
   # minutes.
   com.ibm.cfs.vmc.deployment.deletion.retry.timeout=5
   ```
5. Save the `deployment.properties` file and restart the IBM SmartCloud Entry server.

   Restriction: This function is available only with IBM SmartCloud Entry 2.2 FP 2 or later installed.

Configuring images with VMware

This section describes some additional setup and configuration considerations when using the VMware cloud manager.

VMware considerations when deploying an image

- IBM SmartCloud Entry requires the vCenter virtual switches and port groups to be defined by the VMware vSphere Client before deploying instances. IBM SmartCloud Entry users and administrators are allowed to choose which virtual network the instance uses. IBM SmartCloud Entry supports either standard VMware vSwitches and port groups or VMware distributed virtual switches.

  If you are using a distributed virtual switch, check the type in vCenter to ensure that it is supported. To check the type, follow these steps:

  1. Browse to `https://<your vCenter>/mob`.
  2. Log in with an administrator account.
  3. Select the content link.
  4. Select the root folder.
  5. Select the data center that contains the third party distributed virtual switch.
  6. Select the network folder.
  7. Select the distributed switch that you want (the id starts with **`dvs-`**).

  The top of the page shows the managed object type of the switch. If the switch type is *VmwareDistributedVirtualSwitch* then it is supported. If the type is *DistributedVirtualSwitch* then it is not supported and you receive an error when you deploy to a port group that uses that distributed switch.

- IBM SmartCloud Entry connects to the vCenter server by using a single user ID and password. It is recommended that this user has the vCenter administrator role. If you choose to use a different user ID, that user must have sufficient permissions to perform the operations on the virtual machines. The user ID must also have access to various virtual machine resources, such as networks and datastores.
- Do not change a virtual machines UUID in the vSphere Infrastructure Client. In some cases, such as manually moving a virtual machine, the vSphere Infrastructure Client asks if you want the UUID changed. When an instance is deployed, IBM SmartCloud Entry keeps the UUID of the virtual machine in its database and uses that UUID to find the virtual machine in vCenter, therefore you should not change the UUID.
- At some point, you might decide to migrate from IBM SmartCloud Entry to the IBM Tivoli Service Automation Manager (TSAM) product or other IBM cloud product. To ease the transition, it is highly recommended that you set up your Windows and Linux guest images as required by TSAM. Even if you have no plans to migrate, see Creating operating system image templates for VMware in the IBM Tivoli Service Automation Manager information center at http://pic.dhe.ibm.com/infocenter/tivihelp/v10r1/topic/com.ibm.tsam_7.2.4.1.doc/rdp/c_supported_os_vmware.html for more information about configuring your guest images.
- It is recommended that you install VMware tools on your guest operating systems before you make the virtual machine a template.
- If you are using the VMware Converter tool to import your virtual machines into vCenter, you should fully start the virtual server by using the VMware vSphere Client before you make it a template. This action allows vCenter to discover whether VMware tools are installed into the guest.
- All virtual machines in vCenter are shown as instances in IBM SmartCloud Entry. If you convert a virtual machine to a template, the status of that instance in IBM SmartCloud Entry changes to Unknown since the virtual machine is now a template. Do not delete this instance from IBM SmartCloud Entry since that deletes the underlying template on vCenter. If you want to make this instance not available for non-administrative users, use the Hide option instead.
- IBM SmartCloud Entry does not allow you to import vApps. If you want to enable users to deploy a single virtual server vApp, follow these steps:
  - Import the vApp by using vCenter
  - Modify the vApp properties as required by the application.
  - Convert the vApp to a template
- vApps with more than one virtual server are not supported.
- During the deployment of an image, IBM SmartCloud Entry uses the VMware API to apply customizations to the new virtual machine image. Therefore the VMware template image must be customizable by VMware. While VMware vCenter enables you to deploy a template without customizations, this option is not available in IBM SmartCloud Entry.
- When you deploy an image, IBM SmartCloud Entry instructs VMware to power on the newly deployed virtual machine. In some cases, depending on server loads, VMware might not power on the virtual machine. In this case, IBM SmartCloud Entry displays, by default, the instance in STOPPED state. Since the instance has been successfully cloned and configured, IBM SmartCloud Entry does not display an error and the instance can be started by the user. You can change this default behavior by using a deployment property that is described in section "VMware wait for deployed virtual machine".
- By default, IBM SmartCloud Entry reports a newly deployed instance in OK state as soon as VMware powers on the virtual machine. Depending on the guest operating system and image definition, it might be a few minutes before the virtual machine is completely up and running and can be used. In some cases, VMware might restart the virtual machine more than once during the customization process. You can change this default behavior by using a deployment property that is described in section "VMware wait for deployed virtual machine".
- IBM SmartCloud Entry allows the target of a deployment to be either a specific host, a host resource pool that is associated with a host, a cluster, or a resource pool that is associated with a cluster. If the cluster is a DRS enabled cluster, VMware chooses the appropriate host and therefore you cannot choose an individual host in that cluster. By default, IBM SmartCloud Entry is configured to randomly

choose a host that is not associated with a cluster. If no hosts are available, you get an error when you deploy. You can change the default behavior by modifying the `deployment.properties` file as described in section “Configuring a deployment target” on page 85. However, it is recommended that an administrator configure each images target. For more information, see “Configuring global image deployment” on page 84.

Saving, restoring, and deleting virtual servers

The IBM SmartCloud Entry allows users to save back up copies of their virtual server disks and configuration files. These copies can be restored later.

In addition, IBM SmartCloud Entry provides functions to allow users to view and delete their saved images. IBM SmartCloud Entry allows users to keep an administrator configured number of saved images. When the limit is reached, the system automatically deletes the oldest saved image. For information about how users perform save, restore, view, and delete operations, see the IBM SmartCloud Entry User Guide.

Deleting a virtual server

When a virtual server is deleted, all the saved images are deleted at the same time. There is no option to keep images beyond the life of the virtual server.

Approvals

The save and restore functions can be configured for approval control. This requires an IBM SmartCloud Entry administrator to first approve any save or restore request.

Note: If the virtual server is powered on, the save function powers down the virtual server before starting the save operation. If the approval process is enabled, the virtual server remains powered on until the administrator approves the save or restore request. There is no approval process for deleting a saved virtual server image. To enable the approval process, see “Approval policies” on page 127.

Authorization

Only the creator of an instance, an IBM SmartCloud Entry administrator, or the project owner is allowed to save, restore, or delete a virtual server image. Users within the same project are not allowed to perform save, restore, or delete operations on other user images within a project.

Notifications

The save, restore, and delete images functions log events to the IBM SmartCloud Entry event log. In addition, save image and restore image operations send email notifications, if the user configuration is enabled to receive email notifications.

For more information about email notifications, see “Configuring email notifications” on page 83.

Setting saved image limit

By default, IBM SmartCloud Entry allows you to keep up to three saved virtual server images.

About this task

To change this limit, follow these steps:

Procedure

1. Open the `deployment.properties` file.
2. Update the `com.ibm.cfs.vs.max.backups` property.

For example, to keep 10 saved virtual server images, change the property to the following setting:

```
com.ibm.cfs.vs.max.backups=10
```

3. Save the `deployment.properties` file.
4. Restart the IBM SmartCloud Entry server.

VMware datastore assignment during deployment

There is a new deployment property that you can set to select the target storage to be used when you deploy a virtual image. You can set the **Target Storage** property value to *datastores* or *datastore clusters* that are attached to the selected deployment target. If the selected deployment target is changed, the target storage value is updated to match what is available on the newly selected deployment target. IBM SmartCloud Entry always sets the default target storage value to use the default storage selection algorithm.

The default storage selection algorithm retrieves the list of datastores and datastore clusters that are associated with the deployment target. It then selects one of the datastores or datastore clusters that is backed by a block device that has enough free space to contain the virtual machine disk sizes. If a block storage cannot be selected, then the appropriate NFS file storage, with the largest free space is chosen. If there is no available storage, the deployment fails.

You can specify a set of datastores and datastore clusters for the selection algorithm to exclude or include or both. Set the `com.ibm.cfs.cloud.vmware.enable.clone.template.properties` property in the `vmware.properties` file to `true`. To exclude datastores and datastore clusters from being selected, edit the `com.ibm.cfs.cloud.vmware.datastore.exclude.list` property and add a comma-separated list of datastore and datastore cluster names. To set the datastores and datastore clusters that can be selected, edit the `com.ibm.cfs.cloud.vmware.datastore.include.list` property and add a comma-separated list of datastore and datastore cluster names.

Note: By default, the selection algorithm includes all of the datastores and datastore clusters that are associated with the deployment target.

For example,

```
com.ibm.cfs.cloud.vmware.enable.clone.template.properties=true
com.ibm.cfs.cloud.vmware.datastore.exclude.list=dscluster3,localdisk4
com.ibm.cfs.cloud.vmware.datastore.include.list=localdisk1,dscluster2
```

To disable the algorithm, specify the datastore that you want to use in the `com.ibm.cfs.cloud.vmware.target.datastore.names` property.

For example:

```
com.ibm.cfs.cloud.vmware.enable.clone.template.properties=true
com.ibm.cfs.cloud.vmware.target.datastore.names=san,san,san
```

Each datastore that is listed is for a different virtual disk. The first entry is the datastore where the virtual server configuration files are located. The subsequent datastores in the list are for the virtual system hard disk devices. For example, if your virtual server has three disks you must specify four datastores in this list. These datastores can all be the same datastore or a combination of different datastores. If the first entry is for a datastore cluster, then the remaining entries are ignored. The datastore cluster is used for both the configuration files and disks. Datastore clusters are ignored when specified for subsequent entries in the list.

These `vmware.properties` file changes apply globally to IBM SmartCloud Entry and therefore to all deployment targets. Make sure that you specify datastores and datastore clusters that are available to all hosts that are the potential targets for every image. You cannot use the include list and datastore names properties, if the following is true:

- You have multiple cluster targets, each with its own set of storage, that is managed by the same vCenter.
- You want IBM SmartCloud Entry to target all the clusters.

In the datastore names property, you can specify different datastores for different disks if your virtual server templates have more than one disk.

Note:

- Datastore clusters are only available when you are using vSphere 5 Enterprise Plus edition. For more information about configuring and using datastore clusters, see the vSphere documentation.
- When you create the `vmware.properties` file, you must restart IBM SmartCloud Entry server. However, changes made to the property file after you restart the server are automatically updated.

Setting VMware user data during deployment

When you deploy an image, you can set user data for the deployed virtual machine by using instance customization. The user data customization enables you to pass your own configuration information to the deployed virtual machine. If this customization fails during deployment, IBM SmartCloud Entry displays the instance in FAILED state.

About this task

IBM SmartCloud Entry supports base64 encoded and plain text user data. The default value is set to base64 encoded. If decoding the user data fails, the user data is treated as plain text. IBM SmartCloud Entry passes the decoded user data to the deployed virtual machine through a CD backed by an ISO file. This gives the virtual machine access to the user data through the `user-data` file on one of its CD devices.

IBM SmartCloud Entry must be configured properly to create an ISO file that contains the user data. If IBM SmartCloud Entry is installed on Linux or AIX, then the **`mkisofs`** or **`genisoimage`** binary must exist in the `/usr/bin` directory. If IBM SmartCloud Entry is installed on Windows then **`Cygwin`** must also be installed and the `mkisofs.exe` or `genisoimage.exe` executable file must exist in the Cygwin binary path that is specified by the `com.ibm.cfs.cloud.vmware.user.data.iso.cygwin.binary.path` property in the `vmware.properties` file.

In addition, you can also set the following properties in the `vmware.properties` file to control the user data:

com.ibm.cfs.cloud.vmware.user.data.file.name
The name of the file on the ISO that contains the actual user data. The default value is *user-data*.

com.ibm.cfs.cloud.vmware.user.data.iso.temp.path
The name of the path that is used to temporarily store ISO files on the IBM SmartCloud Entry server. The default value is the IBM SmartCloud Entry home directory. This path must end with a path separator, such as '/' on Linux and '\' on Windows.

com.ibm.cfs.cloud.vmware.user.data.iso.cygwin.binary.path
The name of the path to the Windows Cygwin binaries. If IBM SmartCloud Entry is installed on Windows then the `mkisofs.exe` or `genisoimage.exe` files must exist in this path. If IBM SmartCloud Entry is installed on Linux or AIX, then this property is not used. The default value is the IBM SmartCloud Entry home directory. This path must end with a path separator, such as '/' on Linux and '\' on Windows.

Note:

- The ISO files that are created are managed by IBM SmartCloud Entry and not VMware. As a result, when you delete a virtual machine outside of IBM SmartCloud Entry, such as through the vSphere client interface, the ISO file that is created for the virtual machine is not removed.

- The ISO file of the virtual machine that contains the user data is not preserved with any saved virtual server images or capture instances that are created from the virtual machine.
- For more information about Cygwin, see cygwin.com.

Set secure access during deployment

When you deploy a Linux image, you can set secure access to the deployed virtual machine by using instance customizations.

Using these optional customizations, you can set the password or SSH public key or both for a user on the guest operating system. If these customizations fail during deployment, IBM SmartCloud Entry displays the instance in FAILED state. You can set secure access for a root or a non-root user.

IBM SmartCloud Entry must be provided with the current root user name and password for the guest operating system to set secure access during deployment. In addition, IBM SmartCloud Entry uses VMware guest operations to complete the customizations and there are special requirements for performing VMware guest operations. For more information, see "Requirements for VMware guest operation" on page 95.

When you set a password for a user, access the IBM SmartCloud Entry server by using a secure connection. This ensures that the password is encrypted when sent to the IBM SmartCloud Entry server. For more information, see "IBM SmartCloud Entry for Cloud SSL configuration (optional)" on page 31.

When you set an SSH public key for a user, the guest operating system must have OpenSSH installed and configured to take advantage of this customization. In addition, the SSH public key must be specified according to the OpenSSH authorized_keys file format. For more information about OpenSSH, see http://www.openssh.org/.

Resetting secure access during capture

When you capture a Linux instance, the SSH public keys for a user are removed from the guest operating system if they were set by IBM SmartCloud Entry when the instance was deployed.

Note: For more information, see "Set secure access during deployment."

Removing the SSH public keys prevents the keys from being available to instances deployed from the captured image. If the SSH public keys are unable to be removed during capture, IBM SmartCloud Entry displays warning messages in the image logs. In such cases, you must manually remove the SSH public keys for the user.

IBM SmartCloud Entry needs the current root user name and password for the guest operating system to reset secure access during capture. IBM SmartCloud Entry obtains this information from the virtual server credentials, which are initially set based on the instance customizations. The virtual server credentials can be reset later if changed in the guest operating system after deployment. For more information, see the *GET* and *PUT /instances/{id}/virtualServers/{id}/credentials* REST APIs in the IBM SmartCloud Entry Software Development Kit (SDK) Reference guide.

IBM SmartCloud Entry uses VMware guest operations to reset secure access during capture and there are special requirements for performing VMware guest operations.

Note: For more information, see "Requirements for VMware guest operation" on page 95.

Waiting for a deployed virtual machine (VMware)

IBM SmartCloud Entry provides a deployment property that enables users to specify whether to wait for a deployed virtual machine to be started and ready for use before it reports the newly deployed instance in OK state.

About this task

This deployment property option is labeled “Wait for the deployed virtual machine to be started and ready for use.” When this option is enabled, IBM SmartCloud Entry displays the instance in a FAILED state, if the deployed virtual machine is not started and ready for use in the allotted time. A failure can be caused by problems during the customization process (for example, specifying an incorrect Windows product key) or if the virtual machine cannot be powered on.

If VMware Tools is installed on the guest operating system, the virtual machine is considered started and ready for use when the virtual machine is powered on and the necessary network customizations are completed for it. If VMware Tools is not installed, then only the powered on state is checked.

You can configure the amount of time to wait for a deployed virtual machine to be started and ready for use by setting the *com.ibm.cfs.cloud.vmware.deployed.vm.start.wait.time* in the `vmware.properties` file. The time is in seconds and defaults to 2,700 (or 45 minutes). For example, *com.ibm.cfs.cloud.vmware.deployed.vm.start.wait.time=1800*

You can also configure the default value for this deployment property by setting *com.ibm.cfs.cloud.vmware.default.deployed.vm.start.wait* in the `vmware.properties` file. The default value is *false*, which disables the option so that IBM SmartCloud Entry reports a newly deployed instance in OK state as soon as VMware powers on the virtual machine. You can override the *com.ibm.cfs.cloud.vmware.default.deployed.vm.start.wait* setting when you configure or deploy an image. For example, *com.ibm.cfs.cloud.vmware.default.deployed.vm.start.wait=true*.

Note:

- The wait time starts after IBM SmartCloud Entry attempts to power on the deployed virtual machine.
- This deployment property applies globally to IBM SmartCloud Entry and therefore to all VMware deployments.
- When you create the `vmware.properties` file, you must restart IBM SmartCloud Entry server; however changes made to the property file after that are picked up automatically.
- During deployment, some optional instance customizations require the deployed virtual machine to be started and ready for use before the customizations can be completed. In such cases,IBM SmartCloud Entry waits for the deployed virtual machine regardless of the value that is specified for this deployment property.

  Note: For example, see “Set secure access during deployment” on page 94.

Requirements for VMware guest operation

VMware guest operations are used to perform certain optional customizations of instances.

When you request such customizations, your request must meet the following requirements to successfully perform the VMware guest operations:

1. vCenter version 5.0 or later is required.
2. The host machine that is used for the instance must be at version 5.0 or later and IBM SmartCloud Entry must have network connectivity to it.
3. VMware tools must be installed and current on the guest operating system for the virtual machine.
4. VMware guest operations must be enabled for both the virtual machine and the host machine. They are enabled by default, but can be disabled.

Note: If it is necessary to connect to the host machine to complete the VMware guest operations, IBM SmartCloud Entry automatically accepts the security certificate for the host machine. The security certificate is stored in the `<host machine>.jks` file in your IBM SmartCloud Entry home directory.

Configuring shutdown of VMware instances

In previous versions of IBM SmartCloud Entry stopping an active instance of VMware instantly powered off the running instance. The virtual machine was given no delay to allow it to perform its own shutdown process. IBM SmartCloud Entry now provides a 90-second delay for the system to complete the shutdown process. If by the end of 90 seconds the system is not shut down, IBM SmartCloud Entry forces the VMware instance to power down immediately.

You can configure the behavior of how VMware instances are shut down by modifying the following statements in `vmware.properties`:

com.ibm.vmware.client.shutdown.delay.in.milliseconds=90000

This property allows the VMware instance time to shut down before a power off is called. The default is 90000 milliseconds if the property is not specified. Setting this property to `0` (zero) prevents a shutdown from being called.

com.ibm.vmware.client.disable.save.image.shutdown=false

This property disables shutdown when save image is called. The default value is set to `false`, which allows shutdown to be called before save image. Specifying a value of `true` prevents a shutdown from being called on save image operations.

VMware limitations

The following limitations apply to VMware and IBM SmartCloud Entry.

- The saved images are managed by IBM SmartCloud Entry and not VMware. Deleting an image outside of IBM SmartCloud Entry, such as through the vSphere client interface, does not remove the saved images.
- Properties that are defined in the `deployment.properties` file and the `vmware.properties` file are global to all users, instances, and images. There is no option to configure these options on a more granular level.
- If you have an image that is defined in IBM SmartCloud Entry and you rename the associated virtual machine template by using the vSphere Client, the name of the image in IBM SmartCloud Entry does not change. The IBM SmartCloud Entry image is still associated with the renamed template and can continue to be used. The image details page displays the renamed template name in the `Original name` field. You can manually change the name of the image by clicking the name of the image on the Images details page and pressing **Save**.
- If you have an image that is defined in IBM SmartCloud Entry and you convert it to a virtual machine by using the vSphere Client, the image in IBM SmartCloud Entry shows a state of `unknown`. This state is displayed because it is no longer a template on the VMware server; the conversion made it a virtual machine, which shows up as an IBM SmartCloud Entry instance. If the unknown IBM SmartCloud Entry image is no longer needed, it can be deleted. A deletion of the IBM SmartCloud Entry image does not affect the IBM SmartCloud Entry instance or virtual machine on the VMware server.
- In some cases, when you use special characters in names of VMware objects such as port group names and cluster names, the VMware API encodes these specials characters in a URL encoding scheme. For example a `/` character is encoded as a `%2f`. When the names are displayed in IBM SmartCloud Entry, the characters are not decoded. IBM SmartCloud Entry displays the encoded name. For example, if you have a cluster named `DRS/Cluster` it is displayed as `DRS%2f%Cluster`.
- IBM SmartCloud Entry creates and manages custom fields for internal use when using VMware virtual machines. The custom fields have a `"SKC_"` prefix and you should not modify or remove them using the vSphere client.

Configuring images with OpenStack

When an image is deployed, you might have to customize the resulting instance on startup to apply network configurations, login information, application settings, and so on, before the instance is ready for use.

About this task

IBM SmartCloud Entry uses OpenStack config drive support to pass customizations (for example: server metadata, user data, personality files, and SSH keys) to an instance. The config drive can be accessed by any guest operating system capable of mounting an ISO9960 file system. Images that are built with a recent version of the cloud-init software package, or similar software package such as IBM SmartCloud init, can automatically access and apply the supported customizations that are passed to the instance by the config drive.

Note:

- For more information about the cloud-init software package and the customizations that it supports, see CloudInit.
- For more information about the IBM SmartCloud init software package and the customizations that it supports, see Bootstrap a cloud instance with IBM SmartCloud init

IBM SmartCloud Entry also supports the Pluggable Configuration Strategy feature added by IBM to OpenStack. This feature is similar to the config drive support in that it provides an instance with the necessary customizations. Like config drive, the image must be built with the correct software package for the configuration strategy to automatically access and apply the customizations. In particular, this feature provides support for Open Virtualization Format (OVF) or Microsoft Windows System Preparation (Sysprep) configuration. For more information, see the following resources:

- For information about OVF configuration, see Open Virtualization Format (OVF).
- For information about Sysprep configuration, see Sysprep Technical Reference.

Cloud-init software package

IBM SmartCloud Entry supports the cloud-init software package.

When you deploy an image, IBM SmartCloud Entry makes the instance customizations available to cloud-init using the OpenStack config drive support. The cloud-init software package can then access the config drive and apply the customizations to the instance. The following are some of the customizations made available through the config drive:

1. User data
2. Personality files
3. SSH key pair
4. Network adapter information (for static networks)

Using IBM SmartCloud Entry, you can enter the contents of the user data and personality files by using the deployment properties. You can enter the contents when you configure or deploy an image. The contents can be either base64 encoded or plain text. There are also deployment properties for the SSH key pair and network adapters that are based on the SSH key pairs and networks available. You can set the network adapters when you configure or deploy an image. However, the SSH key pair should not be set when you configure an image because OpenStack SSH key pairs are scoped to a user. Instead, the user who deploys the image should select an appropriate SSH key pair.

Note:

- For more information about the cloud-init software package and the customizations that it supports, see CloudInit.
- For more information about the OpenStack config drive support, see Config drive.

Configuration strategies

IBM SmartCloud Entry supports the OVF and Sysprep types of pluggable configuration strategies.

When an image is deployed that has one of these configuration strategies, the OpenStack Pluggable Configuration Strategy feature determines the customizations made available to the instance and how they are made available. The appropriate software package (for the configuration strategy type) on the image is expected to access and apply the customizations. The customizations that are provided by OpenStack come from the following sources:

1. Server metadata that is provided by OpenStack itself.
2. Server metadata that is provided by the user deploying the image.

The following server metadata is provided by OpenStack:

```
server.admin_password              Random administrator password generated by OpenStack.
server.hostname                    The hostname for the instance.
server.domainname                  Domain name from the dhcp_domain configuration option.
server.dns-client.pri_dns          Primary DNS server IP address.
server.network.[n].mac             Mac address for network interface number n.
server.network.[n].mac_alt         Mac address formatted with '-' rather than ':'.
server.network.[n].slotnumber      Slot number for network interface number n.
                                   Defined as the decimal value of the last two digits
                                   of the mac address.
server.network.[n].[v4|v6].address IPv4 or IPv6 address for network interface number n.
server.network.[n].[v4|v6].netmask IPv4 or IPv6 netmask for network interface number n.
server.network.[n].[v4|v6].cidr    IPv4 or IPv6 address and netmask in CIDR notation
                                   for network interface number n.
server.network.[n].[v4|v6].gateway IPv4 or IPv6 gateway for network interface number n.
server.network.[n].v4.use_dhcp     'true' if the network uses DHCP.
```

Server metadata that is provided by the user during deployment are prefixed with 'server.metadata'.

Creating a configuration strategy:

A complete and accurate OVF or Sysprep configuration strategy is important to ensure that an image can be deployed and customized properly. A poor configuration strategy can cause the deployment to fail or prevent the instance from being customized.

About this task

A configuration strategy consists of the following parts:

- Type
- Template
- Mapping
- User metadata

For information about how to add, update or delete the configuration strategy of an image, see "Updating an image configuration strategy (OpenStack only)" on page 118.

Type The type is required and can either be ovf or sysprep.

Template

The template is required. When you are using an ovf configuration strategy type, this contains the OVF descriptor for the image. When you are using a sysprep configuration strategy type, this contains the template unattend.xml file for the image.

Mapping

The mapping is required. It defines how to map the server metadata that is provided by both OpenStack and the user deploying the image to the appropriate elements/parts of the template. The mapping is a JavaScript Object Notation (JSON) array of objects, where each object has a source representing the server metadata to map to the target element/part in the template. For example:

```
[
  {
    "source": "server.network.1.v4.address",
    "target": "com.ibm.vsae.2_1.network-interface.ipaddr"
  },

  {
    "source": "server.network.1.v4.netmask",
    "target": "com.ibm.vsae.2_1.network-interface.netmask"
  },

  {
    "source": "server.network.1.v4.gateway",
    "target": "com.ibm.vsae.2_1.network-interface.gateway"
  },

  {
    "source": "server.hostname",
    "target": "com.ibm.vsae.2_1.system-host.hostname"
  },

  {
    "source": "server.domainname",
    "target": "com.ibm.vsae.2_1.system-host.domainname"
  },

  {
    "source": "server.dns-client.pri_dns",
    "target": "com.ibm.vsae.2_1.dns-client.pri_dns"
  },

  {
    "source": "server.metadata.username",
    "target": "com.ibm.vsae.2_1.system-user.username"
  },

  {
    "source": "server.metadata.system.password",
    "target": "com.ibm.vsae.2_1.system-user.password"
  }
]
```

IBM SmartCloud Entry uses the mapping to create additional deployment properties for the image. Every object in the mapping with a source prefix of `'server.metadata.'` is added to the configurable deployment properties for the image. Doing so allows such properties to be customized by the user when the image is deployed. For more information about defining the mapping, see “OVF configuration strategy” on page 100 and “Sysprep Configuration Strategy” on page 102 topics.

Note:

- The same source can be mapped to multiple targets. To do this, you must define a separate source/target object in the JSON array for each mapping.
- An empty mapping (for example, []) must be used only for testing purposes since all deploys will use the same template and thus have the same customizations applied.
- When you define a source mapping name with the `'server.metadata.'` prefix, avoid using `'.'` in the suffix portion of the name.

User Metadata

The user metadata is optional. It determines how IBM SmartCloud Entry defines, displays, and processes the configurable deployment properties created based on the mapping. If no user metadata is provided for a mapping, a basic string deployment property is used. Defining detailed user metadata helps users properly configure and deploy the image. The user metadata is a JSON array of objects where each object might contain the following:

1. name
2. type

3. subtype
4. description
5. required
6. min
7. max
8. allowed_values
9. default_value

For example:

```
[
 {
  "name": "system.username",
  "type": "STRING",
  "description": "System user name",
  "required": "true"
 },
 {
  "name": "system.password",
  "type": "STRING",
  "subtype": "PASSWORD",
  "description": "System user password hash",
  "required": "true"
 }
]
```

The name string is required. The name corresponds to the mapping source without the `'server.metadata.'` prefix.

The type string is optional. It is the native type of the deployment property (INT, LONG, FLOAT, BOOLEAN, or STRING). The default is *STRING*.

The subtype string is optional. It is a more descriptive type to allow for early validation of the deployment property. A STRING type can have the following subtypes: *IPV4_ADDRESS, DOMAIN_NAME, DOMAIN_NAMES, IPV4_SUBNET_MASK, HOST_NAME and PASSWORD.* A BOOLEAN type can have the following subtypes: *DHCP_FLAG* and *DNS_FLAG*. The default is no specific subtype.

The description string is an optional description of the deployment property. If no description is provided, the name is used for the description.

The required flag is optional. It is a flag indicating whether the deployment property is required when deploying the image. The default is false.

The min and max strings are optional. They provide minimum and maximum boundaries for *INT, LONG, FLOAT* and *STRING* type deployment properties. The default is no boundaries.

The *allowed_values* string is optional. It is a comma-separated list of allowed values for the deployment property. When you specify a list of allowed values, also provide the *default_value* and ensure that the allowed values are valid for the type. The default is any allowed values corresponding to the type.

The *default_value* string is optional. It is the default value for the deployment property. The default value should be valid for the type. If no default value is provided, a value must be explicitly set by the user in order for the deployment property to be used when deploying the image.

OVF configuration strategy:

The OVF configuration strategy is an example of an OpenStack Pluggable Configuration Strategy. It is designed for use with OVF configuration, which is a way to package and provide configuration options for an image.

About this task

The OVF configuration strategy supports OVF version 1.1. For more information about OVF standards, see Open Virtualization Format (OVF).

The OVF configuration strategy passes the configuration options in an `ovf-env.xml` file in a disk that is presented to the guest system. It is expected that an activation engine, such as IBM VSAE, embedded in the image mounts the drive, read the `ovf-env.xml`, and apply the customizations when an instance deployed from the image starts.

The `ovf-env.xml` file is created based on the default values in the OVF descriptor (that is, the template in the configuration strategy) and the configuration options that are mapped using the mapping that is specified in the configuration strategy.

To know what mappings to specify in the configuration strategy, you must know the properties that the image expects in the `ovf-env.xml` file. The properties that the image expects in the ovf-env.xml are specified in the OVF descriptor's ProductSection elements, as documented in the OVF 1.1 specification, section 9.5. Here is an example ProductSection from an OVF descriptor:

```
<ovf:ProductSection ovf:class="com.ibm.vsae.2_1.network-interface">
 <ovf:Info>System network interface configuration</ovf:Info>
 <ovf:Property ovf:key="ipaddr" ovf:type="string" ovf:userConfigurable="true"
  ovf:value="192.168.71.129">
  <ovf:Description/>
  <ovf:Label>IP address</ovf:Label>
 </ovf:Property>
</ovf:ProductSection>
```

Using the above example, the image can have a property *com.ibm.vsae.2_1.network-interface.ipaddr* that defaults to *192.168.71.129*. You might want to have the IP address set to the value that OpenStack assigns to it, which is given in the *server.network.1.v4.address* server metadata. To do this, you would create the following mapping:

```
{
 "source": "server.network.1.v4.address",
 "target": "com.ibm.vsae.2_1.network-interface.ipaddr"
}
```

Here is another example ProductSection:

```
<ovf:ProductSection ovf:class="com.ibm.vsae.2_1.ntp-client">
 <ovf:Info>activates the openntp client</ovf:Info>
 <ovf:Property ovf:key="ntp-server" ovf:type="string" ovf:userConfigurable="true"
  ovf:value="0.pool.ntp.org">
  <ovf:Description>Ntp server</ovf:Description>
  <ovf:Label>Ntp server</ovf:Label>
 </ovf:Property>
</ovf:ProductSection>
```

Using the above example, there is no OpenStack provided server metadata that contains the NTP server's IP address. Therefore, if you want users to be able to override the value when they deploy the image, you would create the following `'server.metadata.'` mapping:

```
{
 "source": "server.metadata.ntp-server",
 "target": "com.ibm.vsae.2_1.ntp-client.ntp-server"
}
```

Note: The OVF configuration strategy has the following limitations:

- The OVF configuration strategy support is only for image activation (that is, ProductSection elements) and does not support actions such as adding disks to the image.

- After activation is complete, OpenStack does not automatically detach the disk drive that contains the `ovf-env.xml` file.
- Extensions to IBM VSAE may be required to support network configurations with both IPv4 and IPv6 addresses.

Sysprep Configuration Strategy:

The Sysprep configuration strategy is an example of an OpenStack Pluggable Configuration Strategy. It is designed for use with Microsoft Windows System Preparation (Sysprep) configuration, which allows customizing many aspects of a Windows system as it starts. For more information about Sysprep, see Sysprep Technical Reference.

The Sysprep configuration strategy passes the image configuration options in an unattend.xml file in a CD-ROM device that is presented to the guest system. Before adding the Sysprep configuration strategy to an image, it is expected that the image is ready for Sysprep, and that it runs Sysprep to read the unattend.xml file, and apply the customizations when starting an instance deployed from the image.

The unattend.xml file is created based on the default values in the template unattend.xml file (that is, the template in the configuration strategy) and the configuration options that are mapped using the mapping that is specified in the configuration strategy. To know what mappings to specify in the configuration strategy, you must know the properties that the image expects in the unattend.xml file.

The format of the target values in the configuration strategy mapping is as follows:

- To identify an element, the format is an XPATH. In this case, the contents of the element are replaced with the value of the source configuration property.
- To identify an attribute, the format is like XPATH@attribute-name. In this case, the attribute in the element is set to the value of the source configuration property.

For documentation on the XPATH format, see the python documentation. If the path identifies more than one element, only one of the elements are the target element. If the path does not identify an element in the template the boot of the instance fails with an error.

Example template unattend.xml file:

```
<?xml version="1.0" encoding="utf-8"?>
<unattend xmlns="urn:schemas-microsoft-com:unattend">
 <settings pass="oobeSystem">
  <component name="Microsoft-Windows-Shell-Setup" processorArchitecture="amd64"
 xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State">
   <Display>
    <ColorDepth>16</ColorDepth>
    <HorizontalResolution>1024</HorizontalResolution>
    <RefreshRate>60</RefreshRate>
    <VerticalResolution>768</VerticalResolution>
   </Display>
   <RegisteredOrganization>OpenStack</RegisteredOrganization>
   <OOBE>
    <HideEULAPage>true</HideEULAPage>
    <NetworkLocation>Cluster</NetworkLocation>
    <ProtectYourPC>1</ProtectYourPC>
    <SkipMachineOOBE>true</SkipMachineOOBE>
    <SkipUserOOBE>true</SkipUserOOBE>
   </OOBE>
  </component>
 </settings>
</unattend>
```

Using the above example, the following mapping target would identify the ColorDepth element: *.//{urn:schemas-microsoft-com:unattend}Display/{urn:schemas-microsoft-com:unattend}ColorDepth*

Using the above example, the following mapping target would identify the processorArchitecture attribute in the component element: *.//{urn:schemas-microsoft-com:unattend}component[@name='Microsoft-Windows-Shell Setup']@processorArchitecture*

Considerations for capturing an OpenStack instance

When you capture an instance that was deployed by using a pluggable configuration strategy (OVF or Sysprep), the configuration strategy is copied to the image that was created.

In this case, the activation software (for example, Sysprep or IBM VSAE) already ran and applied the configuration strategy. Therefore, you might have to perform more actions when you capture the instance. If you want the activation software to run again when you deploy the image that was created, the activation software must be reset. If you do not have to run the activation software again, you can delete the configuration strategy from the image that was created. For more information about the reset requirements and other capture prerequisites, see the documentation for the applicable activation software. For more information about pluggable configuration strategies, see “Configuration strategies” on page 97.

Configuring instance resize timeout

IBM SmartCloud Entry allows the administrator to configure a timeout for an instance resize action. This is optional, but can be configured in the event that the cloud manager does not respond in a reasonable timeframe.

About this task

To configure the instance resize timeout, follow these steps:

Procedure

1. Open the `deployment.properties` file in the home directory.
2. Set the `com.ibm.cfs.deployments.resize.timeout` property to the time in minutes to wait for an instance resize action to complete in the cloud. The default value is 10 minutes.
3. Save the `deployment.properties` file and restart the IBM SmartCloud Entry server.

Identifying expired instances

IBM SmartCloud Entry has a configurable task that allows administrators to identify expired instances and how long to keep them after they have expired.

About this task

To set how often expired instances are identified and how long they are kept, follow these steps:

Procedure

1. Open the `deployment.properties` from your home directory.
2. Configure each property in the file.
   a. `com.ibm.cfs.expired.deployments.finder.interval=10`

      When the expiration date is reached, the deployment property is put into an `EXPIRED` state and the virtual machine is stopped in the deployment. The `com.ibm.cfs.expired.deployments.finder.interval` defines how often IBM SmartCloud Entry identifies expired deployments. This interval is set in seconds.

   b. `com.ibm.cfs.deployments.expired.delete.interval=1`

      This property defines the interval for deleting instances that have been identified as expired. The unit is hour. If not set or valid, the default value is 24 hours.

      This property is also defined by the length of the grace period set when you create an expiration policy for a cloud or a project. For more information, see “Expiration policies” on page 130.

Virtual appliance label translations

The OVF standard inherently supports nationalization of appliance labels for customization properties. VMControl does not support this part of the OVF standard. However, IBM SmartCloud Entry allows users to localize their appliances, in what is called the OVA Translations feature.

In order to use the OVA Translations feature, you need to create a `.properties` file and copy it to a subdirectory in the home directory called */ova-translations* This `.properties` file contains translations for customization property labels within an appliance. IBM SmartCloud Entry translates the customization properties labels into the labels provided in the file, based on the locale of the user that is invoking the appliance.

The file is named based on two things:

- Appliance ID
- Translation locale code

The appliance ID can be obtained from VMControl, and it similar to this: `194e28df-12d9-4c43-a146-5cc34046edb`. The locale code is then added to the end of the appliance name, similar to this: `194e28df-12d9-4c43-a146-5cc34046edb_en_US`. This string becomes the name of the `.properties` file, for example `194e28df-12d9-4c43-a146-5cc34046edb_en_US.properties.`

To find the appliance ID, run the following command:

```
GET https://<director>:8244/ibm/director/rest/VMControl/virtualAppliances/<appliance-id>
```

where *appliance-id* is the path to the appliances.

The actual contents of the properties file are a set of key value pairs, where the key is the name of the customization property, and the value is the label translated in the locale specified in the file name. The following code shows some examples:

```
product.AIX1.com.ibm.ovf.vim.2.system.hostname=(Chinese)
product.AIX1.com.ibm.ovf.vim.2.system.hostname.category=TCP/IP (Chinese)
```

IBM SmartCloud Entry assumes that the default locale of the IBM SmartCloud Entry instance is the default locale of the OVF properties and therefore does not translate those. For example, if the IBM SmartCloud Entry instance is running in English and an appliance is requested for a user whose locale is English, then IBM SmartCloud Entry does not translate the appliance properties using this method. If the OVF is not in English, the appliance does not appear translated.

You can configure global values of this form for each locale in the `ova-general-translations` folder. For example:

```
\.skc\ova-general-translations\customization_es.properties
```

You can add appliance-specific properties that overwrite any global values that are set:

```
.skc\ova-translations\194e28df-12d9-4c43-a12d9-4c43-a146-5cc34046edb_en_US.properties
```

Configuring multiple instances for a single deployment

You can deploy multiple instances through a single deployment.

About this task

If you enable the multiple instance deployment function, a user can deploy multiple instances through a single deployment. The deployed instances use the deployment name as the prefix of each single instance. The new names also use **`-x`** as the suffix, where **`x`** is the index of that instance.

Procedure

1. To enable or disable this feature, set the following property value within the `deployment.properties` file that is located in the `/.SCE31` directory:
   - **`com.ibm.cfs.deployments.multi.enabled=true`** to enable the function.
   - **`com.ibm.cfs.deployments.multi.enabled=false`** to disable the function.

   Note: By default, this feature is enabled.
2. To control the maximum number of instances that a user is allowed to deploy at one time, set the following property value within the `deployment.properties` file:

   `com.ibm.cfs.deployments.multi.max.value=5`

   Note:
   - The default value is 5.
   - If this value is set too high, it might overload the connected cloud.

Configuring logging

Log files are automatically saved by IBM SmartCloud Entry. You can configure the default number of log files saved and the types of messages that are logged.

About this task

By default, IBM SmartCloud Entry saves 9 log files of 50 MB each. These defaults can be modified in the `logging.properties` file located in the home directory.

To change the default logging options:

Procedure

Open the `logging.properties` file in the home directory.

- To change the number of log files saved, set the `java.util.logging.FileHandler.count` property to the number of log files that you to save. The default is `9`.
- To change the types of messages saved, set the `java.util.logging.FileHandler.level` property to the level of messages that you want to receive. The default is `INFO`.

  The types of messages that are logged in the log file are informational, warning, and error messages. Use the debugging messages only for troubleshooting and debugging purposes, because performance can be impacted by excessive logging.

What to do next

Modifying the `logging.properties` file requires restarting the IBM SmartCloud Entry server to pick up the changes.

For more information about logging, see Chapter 17, “Troubleshooting,” on page 155.

Configuring a network

IBM SmartCloud Entry provides a convenient way to manage and apply network settings by using network configurations. Network configurations are a group of network settings for a particular environment, typically a virtual network. These settings can be managed as a single entity and applied to image configurations or instance deployment settings.

For example, suppose that a cloud environment contains two virtual networks applicable to instance deployment: a public and a private virtual network. In this case, an administrator might create two network configurations, one for the public and one for the private. In the public configuration, the administrator would specify all the public network settings such as primary DNS, secondary DNS, and primary gateway. The same would be done for the private network configuration. After the configurations are created, the administrator can configure the images to use the appropriate network configuration. This action saves time by not requiring the administrator to specify each network setting in each image. It also allows an easier way to manage the network settings on a virtual network.

While the actual settings specified in a configuration are tailored to a specific environment, the network configurations themselves are a superset of all network settings regardless of image, operating system, or cloud management system. Therefore, all settings that are specified in a configuration are applicable. For example, the primary and secondary WINS settings of a network configuration are only applicable to Windows based images. So when you create a configuration for an image that is not using Windows, these values are not needed and can be left blank.

Note: With the IBM SmartCloud Entry web interface, you can specify the network configuration for a cloud. The web interface displays only the fields that are applicable for that cloud. Before you can create an OpenStack network configuration, you must select an existing OpenStack cloud.

When network configuration settings are applied to either an image configuration or during an advanced instance deployment, their individual settings can be overridden or manually specified, if wanted.

Note: You cannot override or manually specify OpenStack network configuration settings.

You can modify your network connections through the web interface or though the property files in the home directory. For more information about modifying your network connections through the web interface, see "Network configurations" on page 134.

Note: You cannot use property files to specify OpenStack network configuration settings. You must use the IBM SmartCloud Entry web interface.

To modify your network connections from the home directory, create a `.properties` file and save it to your home directory. The name of these files should be prefixed with `networkConfiguration` followed by an arbitrary suffix and the `.properties` file extension, similar to `networkConfiguration.properties`, `networkConfiguration-vlan1.properties`, or `networkConfiguration3.properties`.

Each property file contains a group of network setting. For example, assume that there is a file named `networkConfiguration.properties` in the home directory, which containing the following settings:

```
name=VLAN1
dns1=9.10.244.100
dns2=9.10.244.200
gateway1=9.5.40.1
gateway2=9.5.40.2
domain=mydomain.company.com
subnet=255.255.252.0
networkId=[Network 1]=hostVnet:ETHERNET0/1
useDHCP=false
hostnamePrefix=sce
computerNamePrefix=sce
workgroup=workgroup
description=default network configuration
9.5.42.250
9.5.42.251
9.5.43.23
```

Note: When you use a brocade switch, you must configure a host name prefix in the `networkConfiguration.properties` file: `hostnamePrefix=sce`.

When IBM SmartCloud Entry starts, the network configuration named "VLAN1" is added to the network configuration list.

(VMware only) In the VWware environment, the value of the *Network ID* field is the name of a VMware standard switch network, port group name, or distributed port group. A typical VMware network ID is *VM Network*. This value is used to assign the virtual network adapter to the VMware network during a deployment. The rest of the values in the network configuration should be appropriate for that network. The network configuration displays all available port groups and distributed port groups. Not all port groups or distributed port groups might be available on all target hosts. Validation of this field occurs only at deployment time when the actual deployment target is known. If the selected port group or distributed switch is not available on the selected target host, then an error occurs and the instance deployment fails.

Configuring billing

IBM SmartCloud Entry has a configurable billing and accounting interface that allows IBM SmartCloud Entry to monitor resource use and create subsequent billing to IBM SmartCloud Entry user accounts for the usage.

For more information about accounts, see “Accounts” on page 145.

Configuring billing

To enable billing, edit the `billing.properties` file and define what action to take when an account becomes delinquent. Also, set the time intervals to determine accounts that are delinquent or at their account balance threshold.

About this task

Important: For billing to work, you must also enable metering. Account bills are generated based on metering results.

To configure billing, follow these steps:

Procedure

1. Open the `billing.properties` file in the home directory.
2. Configure each property in the file.

   `com.ibm.cfs.billing.enabled=true`
   Defines whether to enable the billing and accounting functionality in IBM SmartCloud Entry. True enables and false disables billing and accounting.

   `com.ibm.cfs.billing.delinquency.policy= com.ibm.cfs.services.billing.policies.shutdown`
   Determines the action IBM SmartCloud Entry takes against existing instances when an account becomes delinquent. Possible values are as follows:

   ```
   com.ibm.cfs.services.billing.policies.destroy
   com.ibm.cfs.services.billing.policies.shutdown
   com.ibm.cfs.services.billing.policies.do.nothing
   ```

   `com.ibm.cfs.billing.delinquency.finder.interval=120`
   This property represents the number of seconds to wait before running a job that examines each account to determine whether the account is delinquent.

   `com.ibm.cfs.billing.account.balance.threshold.interval= 24`
   This property represents the number of hours to wait before running a job to find accounts that are at their account balance threshold. The default value of this property is 24 hours or 1 day.

Note: The `billing.properties` file is not configurable through the web user interface.

What to do next

After you enable billing, ensure that you also enable metering. For more information, see "Configuring metering" on page 110.

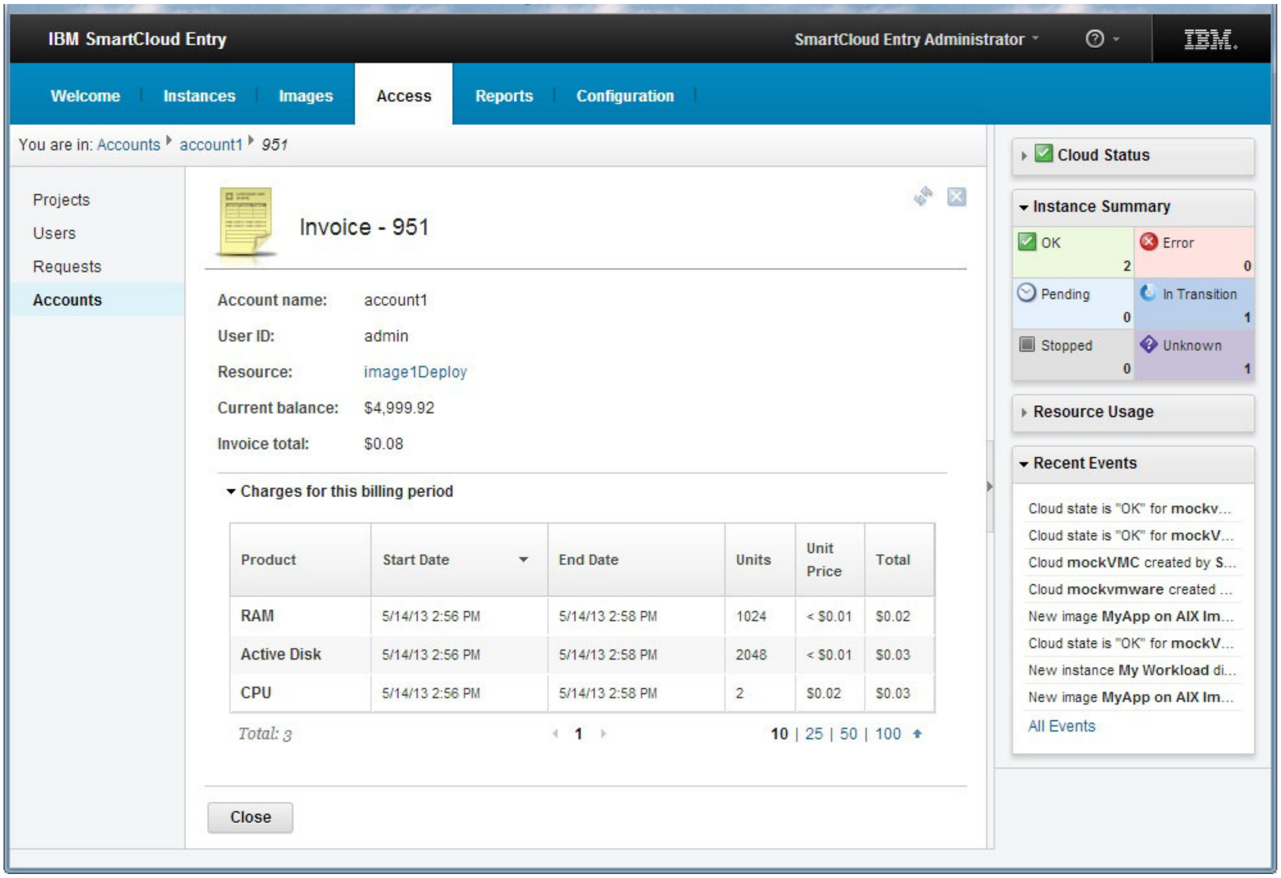
Configuring billing details

IBM SmartCloud Entry can produce charges that are billed back to users when using a specific cloud resource, such as an instance.

About this task

IBM SmartCloud Entry currently has the following configurable products:
- Processor
- Memory
- Disks

A cloud product might be something similar to processor by the hour, 1 GB of RAM per day, a fixed rate charge for a running VM, 20 GB of active disks per day, and so on. IBM SmartCloud Entry loads those cloud products into a product catalog. System events, such as deploying an instance, can cause the creation of a bill with one or more charges from one or more cloud products. IBM SmartCloud Entry automatically deducts money from the account to which the instance owner belongs.



Invoice - 951

Account name: account1
User ID: admin
Resource: image1Deploy
Current balance: $4,999.92
Invoice total: $0.08

Charges for this billing period

Product	Start Date	End Date	Units	Unit Price	Total
RAM	5/14/13 2:56 PM	5/14/13 2:58 PM	1024	< $0.01	$0.02
Active Disk	5/14/13 2:56 PM	5/14/13 2:58 PM	2048	< $0.01	$0.03
CPU	5/14/13 2:56 PM	5/14/13 2:58 PM	2	$0.02	$0.03

Total: 3 ‹ 1 › 10 | 25 | 50 | 100

Cloud state is "OK" for mockv...
Cloud state is "OK" for mockV...
Cloud mockVMC created by S...
Cloud mockvmware created ...
New image MyApp on AIX Im...
Cloud state is "OK" for mockV...
New instance My Workload di...
New image MyApp on AIX Im...

Figure 1. Sample billing account summary

The settings for product price per interval time are configurable. To configure product pricing information, follow these steps:

Procedure

1. Open the `products` directory in the home directory. There are three product configurations: `cpu.xml`, `ram.xml`, and `disk.xml`.
2. Configure processor price in `cpu.xml`.

   ```
   <pricing currency="USD" interval="3600" price="1.000"/>
   ```

   This property specifies that the default IBM SmartCloud Entry collector collects charges on virtual servers using the number of processors that are assigned to them at a rate of $1.00 per hour. Collecting at an interval less than the actual described rate (for example, hours instead of days) enables users to get a more accurate approximation of their actual charges. Having an accurate look at the charges might be important for accounting purposes or in situations where account credit is limited.
3. Configure Memory price in `ram.xml`.

   ```
   <pricing currency="USD" interval="3600" price="0.000976563"/>
   ```

   This property specifies that the default IBM SmartCloud Entry collector collects charges on virtual machines using the number of bytes of RAM assigned to them at a rate of $0.000976563 per MB per hour, which is about $1.00 per hour per GB.
4. Configure disks in `disk.xml`.

   ```
   <cloudProduct id="com.ibm.cfs.cloud.vmc.products.storage">
   <name>Active Disk</name>
   <description>The amount of total disk storage in MB used in a workload
   per hour.</description>
   <!-- $0.000976563 per megabyte per hour = ~$1.00 hour per GB. -->
   <pricing currency="USD" interval="3600" price="0.000976563"/>
   </cloudProduct>
   ```

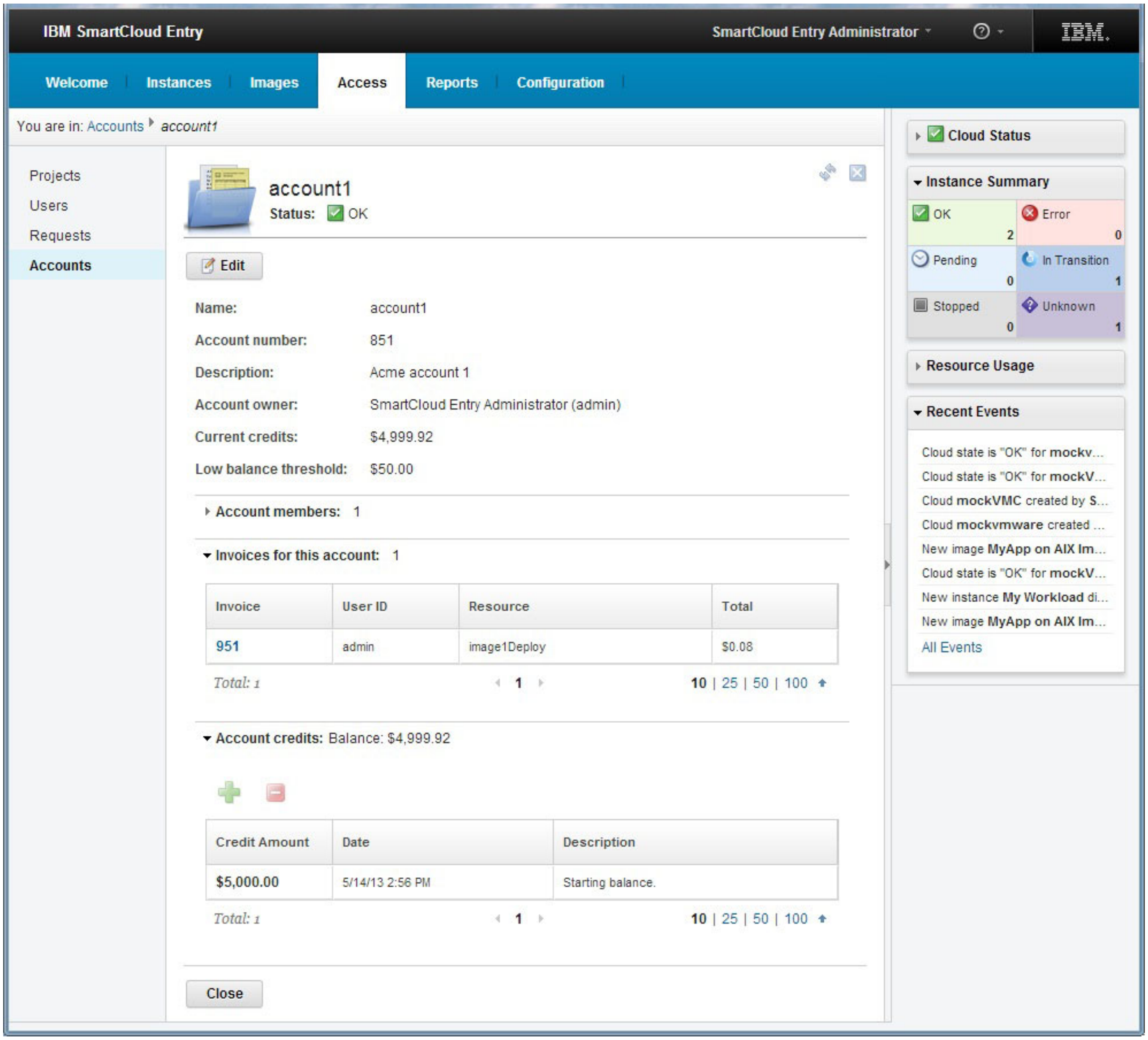
   These properties specify that the default IBM SmartCloud Entry collector collects charges on virtual machines using the disks that are assigned to them at a rate of $0.000976563 per MB per hour, which is about $1.00 per hour per GB.

   The `<name>` and `<description>` can also be overridden from the IBM SmartCloud Entry defaults by specifying different values.

   Note: The currency for all configurable products must be consistent; for example, set US dollar (USD) for both or Chinese Yuan (CNY) for both. Using inconsistent currencies causes incorrect product charges.

Results

After you configure account billing, you can view account billing information in the IBM SmartCloud Entry interface.


IBM SmartCloud Entry
SmartCloud Entry Administrator
IBM.
Welcome
Instances
Images
Access
Reports
Configuration
You are in: Accounts ▸ account1
Projects
Users
Requests
Accounts
Cloud Status
Instance Summary
OK 2
Error 0
Pending 0
In Transition 1
Stopped 0
Unknown 1
Resource Usage
Recent Events
Cloud state is "OK" for mockv...
Cloud state is "OK" for mockV...
Cloud mockVMC created by S...
Cloud mockvmware created ...
New image MyApp on AIX Im...
Cloud state is "OK" for mockV...
New instance My Workload di...
New image MyApp on AIX Im...
All Events
Edit
Close

account1
Status: ✓ OK

Name:	account1
Account number:	851
Description:	Acme account 1
Account owner:	SmartCloud Entry Administrator (admin)
Current credits:	$4,999.92
Low balance threshold:	$50.00

▸ Account members: 1

▾ Invoices for this account: 1

Invoice	User ID	Resource	Total
951	admin	image1Deploy	$0.08

Total: 1 ◂ 1 ▸ 10 | 25 | 50 | 100

▾ Account credits: Balance: $4,999.92

Credit Amount	Date	Description
$5,000.00	5/14/13 2:56 PM	Starting balance.

Total: 1 ◂ 1 ▸ 10 | 25 | 50 | 100

Figure 2. Sample billing account settings

Configuring metering

IBM SmartCloud Entry has a configurable metering framework that enables IBM SmartCloud Entry to record and present metering data.

About this task

You can download metering data files through the metering data API. To enable metering with IBM SmartCloud Entry, configure the following properties:

Procedure

1. Open the `metering.properties` file in the home directory.
2. Configure the property `com.ibm.cfs.metering.enabled=true` to enable the metering function within IBM SmartCloud Entry. The default value for this property is false.

3. Configure the property `com.ibm.cfs.metering.interval=<time in minutes>` where *<time in minutes>* is the time in minutes between each metering record synchronization. The default value is 1441, or every day. If you desire a more frequent synchronization, you can decrease this value.
4. Configure the property `com.ibm.cfs.metering.data.path = cfshome/metricsdata/`. This property allows the administrator to configure the storage system where the metrics data is located. The default location is the IBM SmartCloud Entry `home directory/metricsdata/` if not specified.
5. Configure the property `com.ibm.cfs.metering.data.export.interval = <interval time, hour as unit>`. This property is used for how often to export the metering data to file. The default value is 1 hour.
6. Configure the property `com.ibm.cfs.metering.data.expired.days = <day as unit>`. This property is used to set the number of days that the metering data is expired. The default value is 370 days.
7. Configure the property `com.ibm.cfs.statistics.interval = <interval time, seconds as unit>` This property is used to set the frequency of the synchronization of the statistics resource usage from the cloud. By default, IBM SmartCloud Entry retrieves resource usage from the cloud. These statistics include processors in core, memory, and storage in megabytes. If the property is not set, a default of 60 seconds is used.

Results

After you have configured usage metering, you can monitor the cloud resource usage from the IBM SmartCloud Entry interface by selecting **Reports** > **Usage Metering**. View details about a specific virtual server by selecting the virtual server from the Usage metering grid.

For more information about using Usage Metering, see the IBM SmartCloud Entry User Guide.

Configuring web user interface

Configuring user interface widgets

The widgets in the web user interface of IBM SmartCloud Entry and the properties of the widgets are configurable. Using configuration settings, you can control which widgets appear and in what order they appear.

About this task

To configure user interface widgets for IBM SmartCloud Entry, perform the following steps:

Procedure

1. Open the `web.properties` file in the home directory.
2. Set the `com.ibm.cfs.web.pods.order` property to the names of widgets that are to be shown in the IBM SmartCloud Entry user interface, in the order you want them displayed. The names are not case-sensitive and must be separated by a comma. Possible names include the following names:
   - **CloudStatus**
   - **WorkloadsStatus**
   - **ResourceUsageStatus**
   - **RecentEvents**
3. Set the properties of each widget. The following example shows a widget property configuration example using the CloudStatus widget.
   a. `com.ibm.cfs.web.pods.cloudstatus.enabled=true`

      If the value is *true*, the CloudStatus widget is displayed in the IBM SmartCloud Entry web user interface. If the value is *false*, the property is not specified in the file, or you specify an incorrect value (*truue*) then the CloudStatus widget is not displayed.

b. `com.ibm.cfs.web.pods.cloudstatus.closed`

   If the value is true, the CloudStatus widget is initially displayed in a collapsed form. Otherwise, the CloudStatus widget is initially expanded in the IBM SmartCloud Entry web user interface.

c. `com.ibm.cfs.web.pods.cloudstatus.refresh.interval=30`

   The value of this property indicates how often the CloudStatus widget is refreshed. The value is specified in seconds and must be an integer of 1 or higher.

   Repeat these substeps for each additional named widget to be configured, including WorkloadsStatus, ResourceUsageStatus, and RecentEvents. The following properties can be set:

WorkloadsStatus:

- `com.ibm.cfs.web.pods.workloadsstatus.enabled`
- `com.ibm.cfs.web.pods.workloadsstatus.closed`
- `com.ibm.cfs.web.pods.workloadsstatus.refresh.interval`

ResourceUsageStatus

- `com.ibm.cfs.web.pods.resourceusagestatus.enabled`
- `com.ibm.cfs.web.pods.resourceusagestatus.closed`
- `com.ibm.cfs.web.pods.resourceusagestatus.refresh.interval`

RecentEvents

- `com.ibm.cfs.web.pods.recentevents.enabled`
- `com.ibm.cfs.web.pods.recentevents.closed`
- `com.ibm.cfs.web.pods.recentevents.refresh.interval`

4. Save the `web.properties` file and restart the IBM SmartCloud Entry server. The properties of each widget take effect after the server is restarted.

   Note:

   - If a widget is not listed in `com.ibm.cfs.web.pods.order` and its property `com.ibm.cfs.web.pods.name.enabled` is set to true, it is displayed in the IBM SmartCloud Entry user interface after all the widgets specified in the `com.ibm.cfs.web.pods.order` property.
   - If the `web.properties` file does not exist, all user interface widgets show by default.

Configuring session timeout

You can configure how long a web interface session for an IBM SmartCloud Entry user can remain inactive before the session times out.

About this task

To configure the timeout value, follow these steps:

Procedure

1. Open the `web.properties` file in the home directory.
2. Set the `com.ibm.cfs.client.idle.timeout` property to the number of minutes for which the session is allowed to be inactive. The number must be a positive number and greater than one. After the specified amount of time passes, the user session with IBM SmartCloud Entry expires.

   If the property is set to `-1`, the user session with IBM SmartCloud Entry never expires.
3. Save the `web.properties` file and restart the IBM SmartCloud Entry server. The property takes effect after the server is restarted.

   Note: If `com.ibm.cfs.client.idle.timeout` property is not present or is set to an invalid value, a default value of 30 minutes is used.

Configuring the Welcome page

You can configure IBM SmartCloud Entry to display the welcome page for all users.

Procedure

1. Open the `web.properties` file in the home directory.
2. To display the welcome page for all users, set the `com.ibm.cfs.web.welcomepage.enabled` property to `true`.
3. Save the `web.properties` file and restart the IBM SmartCloud Entry server. The property takes effect after the server is restarted.

   Note: If `com.ibm.cfs.web.welcomepage.enabled` property is not present or is set to an invalid value, the welcome page is displayed.

Configuring the default instance name

You can configure IBM SmartCloud Entry to use a default instance name when deploying an image. If you set this property to true, a default instance name based on the image name that is being deployed is generated; otherwise no default is used.

Procedure

1. Open the `web.properties` file in the home directory.
2. To set the default instance name to the image name being deployed, set the `com.ibm.cfs.web.workloadname.default.enabled` property to `true`.
3. Save the `web.properties` file and restart the IBM SmartCloud Entry server. The property takes effect after the server is restarted.

   Note: If `com.ibm.cfs.web.workloadname.default.enabled` property is not present or is set to an invalid value, the default name is set.

Chapter 13. Configuring IBM SmartCloud Entry from the web interface

This section describes how to use IBM SmartCloud Entry from an administrative viewpoint.

For more information about using IBM SmartCloud Entry as a non-administrative user, see the IBM SmartCloud Entry User Guide.

Configuring the default administrator user account

The default administrator account is created the first time IBM SmartCloud Entry is started. As administrator, configure the default administrator user account to receive email and notification from users.

About this task

To modify the default administrator user account, follow these steps:

Procedure

1. In the IBM SmartCloud Entry interface, log in as the cloud administrator.
2. Select **Cloud Administrator** in the upper right title bar of the screen, and click **Show user preferences**.
3. On the User Profile dialog, enter the administrator email address.
4. Check **Send notifications about instances and other events**.
5. Verify the **Timezone** and **Language** for the administrator.
6. To change the Cloud Administrator password, click **Change Password**.
7. Click **Update.**

Configuring LDAP authentication using the web interface

Use the web interface to configure IBM SmartCloud Entry as an LDAP client.

Procedure

1. Log in to IBM SmartCloud Entry as an administrator.
2. Click the **Configuration** tab and select **LDAP** in the navigation pane.
3. Enter the configuration settings to specify how to connect to the LDAP host.

   Host The fully qualified host name or IP address of the LDAP host.

   Port The port number of the LDAP service on the host. The default is 389.

   Security Protocol
   IBM SmartCloud Entry allows transaction level security (TLS) to be used.

   Certificate
   If transaction level security is used, a certificate must be provided for securing the connection. Consult your LDAP server documentation for details on obtaining the certificate.

   LDAP search DN
   This is the distinguished name that should be used to connect to the LDAP host to perform a directory search, for example cn=Administrator,cn=users,dc=cfs1,dc=us

Note: This field might be required based on the configuration of the LDAP server. If the LDAP search DN is required, the ID must have read authority on the LDAP server.

Password
This is the password that is associated with the LDAP search DN.

Note: This field might be required based on the configuration of the LDAP server.

Search Filter
This is the filter that is used to authenticate users when they log in. Include the special value {FILTER} in the filter to specify where the user ID that is provided during the login should be substituted. For example, (|(userPrincipalName={FILTER}))

Search Context
The search context for providing the LDAP lookup.

User ID attribute
The name of the LDAP field to use as the user ID in IBM SmartCloud Entry.

User name attribute
The name of the LDAP field to use as the user name in IBM SmartCloud Entry.

Email address attribute
The name of the LDAP field to use as the email address in IBM SmartCloud Entry.

4. Click **Save**.
5. Restart the IBM SmartCloud Entry server for the settings to take effect.

What to do next

Notes:

- IBM SmartCloud Entry cannot be returned to use local authentication (non-LDAP authentication) through the web interface. If it is necessary to restore local authentication, see Configuring local authentication for more information. Local authentication is intended only for non-production environments such as for a proof of concept or for performing a demo.
- If you want to enable user name case sensitivity, you must update the `ldap.xml` file after setting the initial LDAP configuration in the web interface. For more information, see “Configuring LDAP authentication manually” on page 78 for more information.

Images

In the **Images** tab, you can manage and configure the images that are available for deployment. You can view image properties and deploy images.

In IBM SmartCloud Entry, each image has a status associated with it. If the status is *OK*, then the image is ready to be deployed. Click the refresh arrow to update the status.

To view the properties of an image, click the name of the image.

If the list of images does not contain the image you want, ensure that the current cloud, project, and architecture filters are set correctly.

Building images

Building images manually is a complex and error-prone process. By pre-building images from specific software bundles for reuse by others, administrators can streamline this process. There are several different ways of building images.

Building images using IBM Image Construction and Composition Tool
Use the Image Construction and Composition Tool to build images for deployment into cloud

environments. You can reuse and manage images and software in a cloud environment. The IBM Image Construction and Composition Tool builds Open Virtualization Appliance (OVA) files that can be deployed into clouds. For more information about the IBM Image Construction and Composition Tool, see Working with IBM Image Construction and Composition Tool at http://pic.dhe.ibm.com/infocenter/tivihelp/v48r1/topic/com.ibm.scp.doc_2.1.0/ICON/topics/iwd_cicn_overview.html and the IBM Redbooks Create Smart Virtual Appliances with IBM Image Construction and Composition Tool at http://www.redbooks.ibm.com/abstracts/sg248042.html.

Building images with VMware Studio

VMware Studio and the OVF Toolkit simplify the process of image creation. The images that are created in VMware Studio can be imported and deployed by using vSphere Client. For more information about using VMware Studio, see VMware Studio Documentation at http://www.vmware.com/support/developer/studio/.

Building images manually

You can choose to build images manually using open source tools. This method requires significant virtualization and image configuration (for example, OVF, Sysprep or cloud-init) experience.

Importing images (OpenStack only)

Using IBM SmartCloud Entry, you can import images to an OpenStack cloud.

About this task

You can create images ready for importing by using tools such as IBM Image Construction and Composition Tool. You can also use existing OpenStack compatible images.

IBM SmartCloud Entry supports OpenStack cloud images in the VHD disk format and for one of the following guest operating systems:

- Windows 8
- Windows 7
- Windows Server 2012
- Windows Server 2008 R2
- Red Hat Enterprise Linux 6.4
- SUSE Linux Enterprise Server 11.2

Note: The imported image file is stored in the OpenStack cloud and not in the IBM SmartCloud Entry database.

Procedure

1. In the IBM SmartCloud Entry interface, click the **Images** tab.
2. Click **More** and choose **Import image...** from the menu to open the Import Image window.
3. Update the cloud, project, image name, disk format, and container format for the image being imported.
4. The image can be imported from a URL or file location. Select the appropriate option and update the image location.
5. Optional: If the image has a minimum memory or storage size requirement, update the memory (MB) and storage (GB) fields accordingly.
6. Click **Import**.

   Note: When you upload an image file using some older browser versions, space for the image file is required in the server `temp` directory. This temporary file is deleted when the upload completes. If the upload does not complete successfully, it is possible that the temporary file is not deleted automatically. If you must use an older browser, place the image file in a location where it can be imported using a URL.

Related reference:

Building images
This topic contains more information about building images.

Related information:

Getting virtual machine images
This site contains example images that are compatible with OpenStack.

Updating an image configuration strategy (OpenStack only)

IBM SmartCloud Entry supports adding, updating, and deleting the configuration strategy for an image in an OpenStack cloud.

About this task

The configuration strategy is stored with the image in the OpenStack cloud.

Procedure

1. Select the image that you want to update.
2. Click **More** and choose **Configuration Strategy...** from the menu.
3. Click **Edit**.

   Note: If a configuration strategy exists, a Delete button is provided to delete the existing configuration strategy. The Edit button can be used to add or update the configuration strategy.
4. Update the configuration strategy type, template, user metadata, and mapping for the image.
5. Click **Save**.

   Note: After you update the configuration strategy, reset the image configuration in order for the updated configuration strategy to be applied when you configure or deploy the image.

Related tasks:

"Configuring images with OpenStack" on page 96
When an image is deployed, you might have to customize the resulting instance on startup to apply network configurations, login information, application settings, and so on, before the instance is ready for use.

Creating a VMware linked virtual machine

Linked virtual machines can be created from a snapshot or from the current running point. A linked clone is a virtual machine whose disks are linked with the template that it was cloned from. Duplicated data is shared between the linked virtual machine and the template. Linked clones deploy much faster because most of the disk data does not have to be copied.

About this task

You can use any image (or template) to create a linked virtual clone. To create a linked virtual clone, follow these steps:

Procedure

1. Open IBM SmartCloud Entry and select **Images**.
2. Select the image that you want to clone and select **Deploy** > **Advanced**.
3. On the Advanced Deployment window, select the option to **Link virtual machine to image**.

What to do next

Note:

- The creation of a linked clone requires the image to contain a virtual machine snapshot. If the image used to create a linked clone does not have a virtual machine snapshot, IBM SmartCloud Entry creates a virtual machine snapshot for the image before the linked clone is created.
- If an image already has a virtual machine snapshot, IBM SmartCloud Entry does not create a new snapshot, but instead uses the current snapshot. Changes that are made to the template might not be reflected, since the clone operation is based on the snapshot and any future changes you make are outside of the snapshot If you must change the template, create a new snapshot that includes your changes.
- Storage DRS supports linked clones starting in VMware vSphere version 5.1. However, Storage DRS is not always able to make a recommendation to place linked clones on a datastore. As a result, an attempt to deploy a linked clone to a storage DRS cluster results in the creation of a full clone, and a warning message in the log that a linked clone was not created.
- The disks of a linked clone cannot be resized. Any attempt to resize a linked disk at deployment time results in an error.
- The datastores of the image must be accessible by the deployment target or the virtual machine cannot be linked to the image. In this case, IBM SmartCloud Entry deploys a full clone.
- You cannot unlink a linked clone from the image.

Configuring image deployment properties

Image deployment customization properties that you want to apply to individual images must be configured through the IBM SmartCloud Entry web user interface. The deployment customization properties are the same properties that are available through a VMControl web interface or CLI deployment. IBM SmartCloud Entry enables you to save these properties in advance so that your users do not have to know all the internal and advanced deployment details.

About this task

To set global image deployment properties, see “Configuring global image deployment” on page 84.

The values that are set in the global image deployment properties are used when deploying an image unless individual deployment properties are set for an image. The values that are set for an individual image are used unless they are explicitly overridden when deploying an image. Administrators can set which values are displayed in the basic deployment or even allow users to set advanced deployment properties. For more information about allowing users to view advanced form, see “Configuring access to advanced deployment form” on page 87.

Note: Global configurations are refreshed only when manually reset or when the deployment target changes.

To configure image default deployment customization properties to be used when deploying it from IBM SmartCloud Entry, complete the following steps:

Procedure

1. In the IBM SmartCloud Entry interface, click the **Images** tab.
2. Click the name of the image that you want to configure.

   Note: If the image that you want is not available, make sure that the correct cloud, architecture, and project are specified.
3. Click **Configure**.

4. Complete the default customization for the image properties. These properties are divided into several groups, including: Hardware, Software, Network, Storage, Image Target and Other Settings, depending on the type of image that you select.

   Note: Changes that were made in the cloud since the image was added, such as networks that were created or removed, might not display on the Configure Image panel. To ensure that the current cloud settings are available to configure the image, click **Reset to Defaults**.

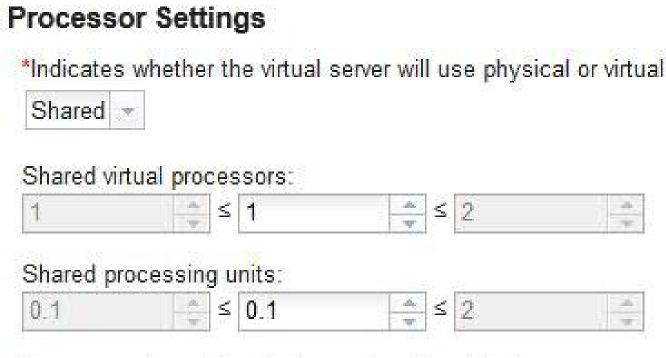
   - Hardware

     Notes:

     – For OpenStack you can control the size of the virtual machine that is deployed from an image by the flavor that you select.

     – For Power Systems that are running in shared mode, the minimum, desired, and maximum number of both shared virtual processors and shared processing units are paired. For each paired value, take care to ensure that values are set correctly. The number of processing units must be less than or equal to the number of virtual processors. However, the processing units, multiplied by 10, must be greater than or equal to the number of virtual processors.

       For example, if the minimum number of virtual processors is 1, then the minimum number of processing units must be less than or equal to 1 (between 0.1 and 1), and must also be greater than or equal to 1 when it is multiplied by 10.



Processor Settings

*Indicates whether the virtual server will use physical or virtual processors (dedicated or shared mode).:

Shared

Shared virtual processors:

1 ≤ 1 ≤ 2

Shared processing units:

0.1 ≤ 0.1 ≤ 2

Figure 3. Processor settings

   - Software
   - Network

     Notes:

     – You can click **Show settings** for each network configuration setting to display configurable options. For Power Systems, VLAN configuration is available in the Adapter network configuration section. (For OpenStack images, **Show settings** is not shown or valid.)

     – The *NONE* value indicates that no network configuration is applied to the settings, in which case the values should be entered manually. (For OpenStack images, *NONE* is not shown or valid.)

     – When a network configuration (including *NONE*) is selected for use, all settings in the subsection are cleared, indicating they draw from the configuration specified.

     – When a network configuration is applied, individual settings can be specified manually by providing a value for the setting and therefore overriding the setting that is specified in the network configuration. Any settings that are blank are taken from the configuration settings. (For OpenStack networks, individual network settings cannot be specified.)

   - Storage

Note: To configure the maximum number of disks that are allowed or the maximum size of the disks, see "Configuring the number and maximum size of additional storage" on page 88.

- Image target
- Other Settings

5. Depending on the image, you might be able to enter the root password for the server that is provisioned by this image, such that users that deploy the image receive the root password in an email notification.
6. Optionally, you can select specific image customization properties to display to a user on the basic deployment form.
   a. Select the **Show basic deploy panel settings** check box at the top of the configuration panel.
   b. For individual customization properties, select the associated **Show in basic deploy settings** check box. This option causes the property to be displayed when a user brings up the basic deployment form for this image. Check only those properties that you want a user to customize, for example, passwords or port numbers for a specific software product included in the image.
7. Select **Save**.

   Note: You can reset an image customization to its original configuration by clicking **Reset to Defaults**.

Deploying an image

You can deploy an image with either basic configuration options or advanced configuration options. Advanced configuration options are only available if the administrator enables them for your environment.

Procedure

1. Click the name of the image you want to deploy.
2. In the Image Details properties page, click **Deploy**.

   Note: The IBM SmartCloud Entry cloud administrator can configure IBM SmartCloud Entry to allow users to use the advanced deployment form when deploying an image. Click **More** > **Advanced deploy** to display the advanced deployment form.

   Basic deployment

   With a basic deployment, minimal configuration options, including name, description, project, flavors (if you are using OpenStack), processor information, memory, and key pairs (if you are using OpenStack and at least one key pair is configured for the user) are displayed.

   Advanced deployment

   Advanced deployment makes a number of different settings available when an image is deployed. For example, with advanced deployment a user can configure setting like networking, storage, and software configuration values. To enable access to these functions, you can do one of the following:

   - Make the advanced deployment form available to all users.
   - Choose specific values for an image by selecting the corresponding check box and exposing that on the basic deployment.

   For more information about enabling advanced deployment options for users, see "Configuring image deployment properties" on page 119.

   With advanced deployment, administrators can configure the options, so users can suspend and resume instances. This option is only visible in a Power Systems virtualization environment. The KVM, VMware, and Hyper-v environments support the suspend action by default. Additionally, in a Power Systems environment, when the target is a server system pool and at least two remote restart capable hosts are added into it, a check box to create a remote restart capable workload is displayed. On KVM, the remote restart capability is enabled by default so the check box does not show up.

If you enable the multiple instances on a single deployment operation, users can deploy multiple instances through a single deployment. The deployed instances use the deployment name as the prefix of each single instance. The new names also use `-x` as the suffix, where `x` is the index of that instance.

If the deployment approval process is enabled, you receive a single approval request. You can change the number of deployment instances while you review the request. The metering and billing functions remain for each of the single deployment instances. When deploying multiple instances on a single deployment, the instances of this deployment are not displayed immediately after you click **Deploy** or **Approve**.

You can also set fields, such as **Virtual Machine Customization**, **Virtual Machine Personality Files**, and more.

Note:

- Only the members of the selected project can see the instance that is created as a result of the image deployment.
- If approvals are enabled, deployment does not begin until the request is approved by the administrator.
- If billing is enabled, you must be a member of an account that is not delinquent for the deployment to proceed.
- The expiration period and approvals policy settings for deployment depends on the policies that are set for the cloud. If more detailed expiration and approvals are set for the project where the image is being deployed, the policies for the project are applied.

Copying image definitions

Rather than copy an entire image, you can create image copies by using just the metadata of the image.

About this task

By copying the metadata, you can make the same image available to multiple projects or provide multiple alternative configurations of the same base image. You can use the Configure Image window to modify various configuration settings for the copies. The copy image function is enabled for administrators and for project owners for images within their project.

When you copy an image definition, only the image metadata that is stored in the IBM SmartCloud Entry database is copied. As a result, any metadata that is stored with the image in the cloud is common across the base and copied images. For example, the configuration strategy for an OpenStack image is metadata that is stored with the image in the cloud. Therefore, the same configuration strategy is used for the base and copied images. For more information about OpenStack configuration strategies, see Configuration strategies.

Note: If you delete the base image, then all copied image configurations are also deleted.

To copy an image definition, perform the following steps:

Procedure

1. On the IBM SmartCloud Entry page, click the **Images** tab.
2. On the Images page, click the base image name that you want to copy.
3. Click **Copy** to enter the image name and description that you want to assign to the copied image.

What to do next

Now you can configure the copied image and move it to different project if desired.

Viewing image properties

You can view image properties such as the image name, description, last modification date, specification version, revision comments, and logs. As an administrator, or if you have project owner authority, you can also make copies of the image, view related images (images that share the same base image), and modify the image name, description, and project.

About this task

Click the image to view or edit the details of that image. Remember that modifications that you make to an image in IBM SmartCloud Entry might not be reflected in the underlying virtualization infrastructure.

Deleting images

Using IBM SmartCloud Entry you can delete images from an OpenStack cloud.

About this task

When you delete an image, it is deleted from IBM SmartCloud Entry and the OpenStack cloud.

The ability to delete an image varies by cloud type:

- IBM Systems Director VMControl and VMware base images can be deleted only if they are in an Unknown state.
- IBM Systems Director VMControl and VMware copied images can be deleted at any time.
- OpenStack images can be deleted at any time. Deleting an OpenStack base image results in all of its related images, or copied images, being deleted as well.

Procedure

1. In the IBM SmartCloud Entry interface, click **Images**.
2. Select the image that you want to delete.
3. Click the delete icon.

Projects

You can create, manage, and request access to projects on the **Projects** page, which is available on the **Access** tab.

Projects are used to define the users that have access to a set of images and instances. Only members of a project can view images and instance within a project. In many cases, projects correspond to a department or other human organization.

To manage projects, go to the **Access** tab and click **Projects** to view the list of available projects.

IBM SmartCloud Entry comes with a default project called the Public project, to which all users belong. All virtual images and instances created outside of the IBM SmartCloud Entry are, by default, assigned to the Public project. You can also configure a staging project to store newly discovered images or instances. The staging project allows administrators to configure images before making them available to other users. For more information, see “Configuring a staging project” on page 86.

Project membership roles

When you are added as a member of a project, one of three membership roles are assigned to you.

Owner
A project owner has administrator authority to the project and its contents. The project owner primarily manages the contents of the project and who has authority to the project and its contents.

User
A project user has the authority to use the project and the objects within the project. For example, a project user can deploy a virtual image to the project. A user can also view and potentially restore backup images of virtual machines created by other users, depending on the way the administrator has set up the project and the roles. The project user primarily handles their own deployments.

Viewer
A project viewer has authority only to view the project and the virtual images and instances contained in the project.

Creating a project

If you are given authority by your administrator, you can create projects.

Before you begin

Discuss your authority level with your administrator. The com.ibm.cfs.project.creation.by.user property in the `deployment.properties` file must be set to True for you to create projects.

Procedure

1. Click **New Project**.
2. Type a project name and description in the corresponding fields.
3. Click **Create**.

Editing project properties

If you have project owner authority, you can edit the properties of an existing project, including project roles, project name, or project membership.

Procedure

1. From the list of projects, select the project you want to edit.
2. To update the project name or description, click the text field and type the new values.
3. To update project membership:
   a. Click **Project Members** to open the panel.
   b. In the Add Project Members window, select the new members and their project roles to add them to the project.
   c. Click **OK**.
   d. To modify an existing member's project role, select the users you want to modify and click **Set Role to** to select the new project role.
   e. To remove members from the project, select the users you want to remove and then click **Remove** to remove the users from the project.
4. To update the expiration policies:
   a. Click **Expiration Policies** to open the panel.
   b. Choose one of the following to set the expiration policy:

      Use cloud default
      The expiration of the deployment will depend on the expiration configuration of the cloud to which the image belongs.

Customize settings
The expiration policy you set on this panel (by setting the **Maximum expiration value** and **Maximum extension period** values) overrides the expiration policy of the cloud to which the image belongs.

5. To update the approval policies:
   a. Click **Approval Policies** to open the panel.
   b. Choose one of the following to set the approval policy:

   Use cloud default
   The project uses the approval policy of cloud groups.

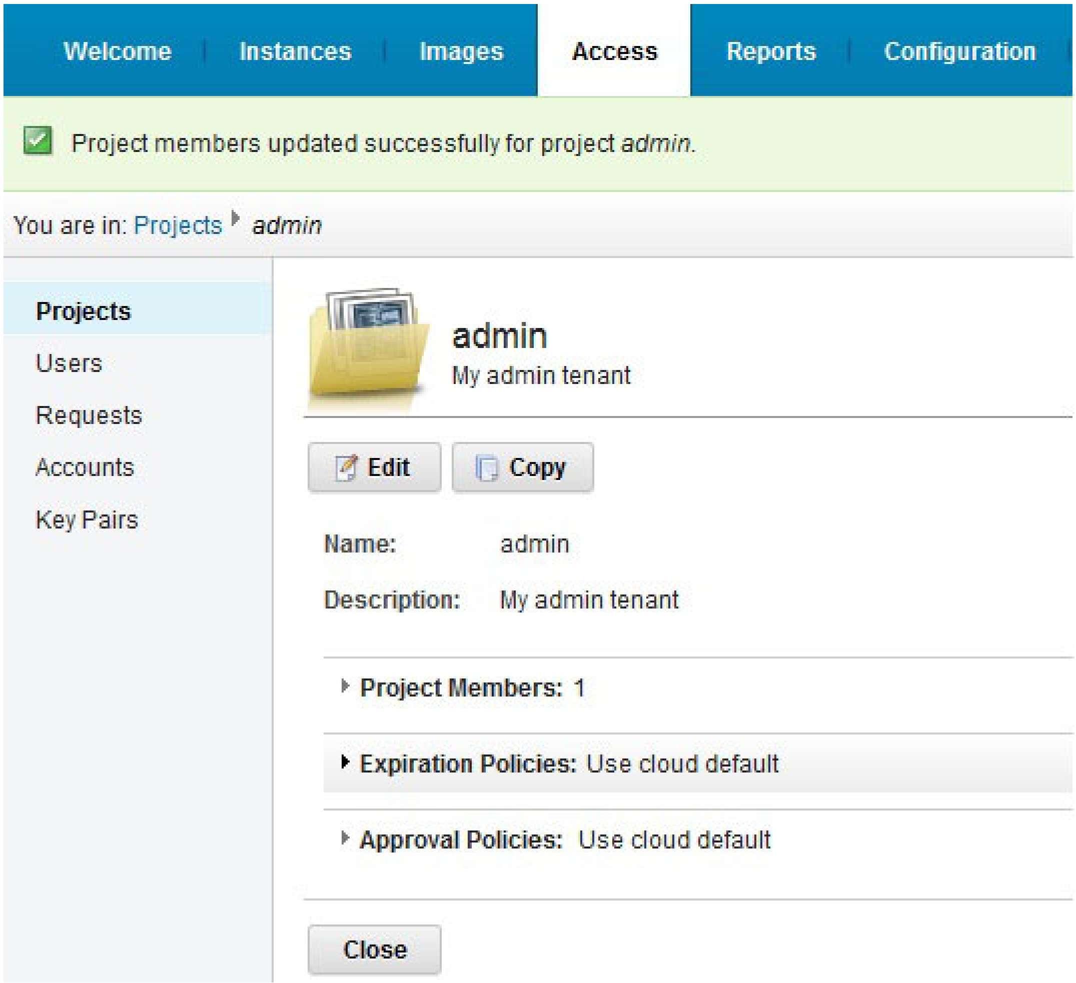
   Customize settings
   The project uses the approval policy you set on this panel (by selecting checkboxes from the **Require approval for the following events** list) overrides the approval policy of the cloud groups.
6. Click **Save**.

Managing projects

For projects that you own, you can set expiration policies and approval policies that affect the instances deployed in that project.

Procedure

1. Click the **Access** tab and then the **Projects** tab.
2. Click the name of the project in the table to display the project properties.
3. Click **Edit**.
4. Expand the title of the item you want to work with: **Expiration Policies** or **Approval Policies**.
5. Set your policies for your projects, or select **Use cloud default** to use the policies set by your administrator.



☑ Project members updated successfully for project *admin*.

You are in: Projects ▸ *admin*

Name: admin

Description: My admin tenant

▸ Project Members: 1

▸ Expiration Policies: Use cloud default

▸ Approval Policies: Use cloud default

Figure 4. Expiration and approval policies

What to do next

For more information about expiration policies and approval policies, see the IBM SmartCloud Entry Administrators Guide.

Deleting an existing project

As a project owner, you can delete a project at any time.

About this task

When a project is deleted from IBM SmartCloud Entry, all of the virtual images and instances contained in the project are transferred to the public project.

Procedure

1. In the projects list, select the project you want to delete.

   Restriction: You cannot delete the default Public project.
2. Click the **Delete selected projects** icon.

Project management with OpenStack

Unlike other cloud types, OpenStack clouds provide native support for project management through the OpenStack keystone component. Because the projects are managed in OpenStack, the projects cannot be updated unless the OpenStack cloud is available.

Keystone is an OpenStack component that provides identity, token, catalog, and policy services to projects in the OpenStack family. Upon first connecting to an OpenStack cloud, IBM SmartCloud Entry imports all the projects that currently exist inOpenStack. The current project membership is accepted and reflected in IBM SmartCloud Entry.

After the initial OpenStack projects import, when connected to an OpenStack cloud, IBM SmartCloud Entry enters transactional mode for project management. When in transactional mode, all project management operations that are performed in IBM SmartCloud Entry are also performed in OpenStack (that is in keystone). If a project management operation (or any of the operations described in this section) fails to complete successfully in IBM SmartCloud Entry it does not occur in OpenStack. Likewise, if it fails in OpenStack, it reverts in IBM SmartCloud Entry.

IBM SmartCloud Entry enters transactional mode for project operations, while connected to OpenStack, in order to have the registries in both products synchronized. For this reason, when connected to an OpenStack cloud, IBM SmartCloud Entry cannot perform project-related operations while the OpenStack cloud is down or unavailable.

To connect to OpenStack, IBM SmartCloud Entry uses a service user account and a default service tenant. Some OpenStack installations have user accounts specific to OpenStack components (for example, nova, keystone, quantum). These and other service user accounts or service tenants in an OpenStack server that do not represent an actual user account or tenant, can be added to the list of service users and service tenants so that they are ignored by IBM SmartCloud Entry. To make this change, add the service users and tenants to the comma-separated list of users in the *com.ibm.cfs.cloud.openstack.service.users* property, or the comma-separated list of tenants in the *com.ibm.cfs.cloud.openstack.service.tenants* property, in the *openstack.properties* file.

Approval policies

IBM SmartCloud Entry administrators can enable approval policy support by specifying the operations that require approval. If approval policies are enabled, the requested operation is held until the approval request is processed by the administrator.

This approval requirement ensures that IBM SmartCloud Entry administrators control the IBM SmartCloud Entry instance process and provides an audit trail of the requester and approver roles.

From a user standpoint, the approval lifecycle behaves similar to the following:

- Users can only see requests that they initiate.
- Users are unable to view any requests against an instance in the public project that they did not originate. Because of this limitation, instances will indicate that they are a Pending state, but users will not be able to see the outstanding requests initiated by other users against that instance.

Setting or modifying approval policies for a cloud

Follow these steps to set or modify an approval policy for a cloud. These policies are used unless they are overridden by an approval policy for a project.

Procedure

1. In the IBM SmartCloud Entry interface, select **Configuration** > **Clouds**.
2. Click the cloud name for which you want to modify approval policies.
3. Select **Approval Policies**.

4. Set the events that require administrator approval.

   Deploying an image
   Approval policy that is invoked when deploying an image to create an instance in the cloud. This approval policy suspends the deployment operation until the generated request is approved or rejected.

   Extending the instance expiration time frame
   Approval policy that is invoked when extending the expiration date of an existing instance. This approval policy suspends the expiration operation until the generated request is approved or rejected.

   Resizing an instance
   Approval policy that is invoked when resizing an existing instance. This approval policy suspends the resize operation until the generated request is approved or rejected.

   Capturing an instance
   Approval policy that is invoked when capturing an existing instance. This approval policy suspends the capturing operation until the generated request is approved or rejected.

   Requesting to attach storage to a virtual machine
   Approval policy that is invoked when attaching storage to a virtual machine. This approval policy suspends the attach storage operation until the generated request is approved or rejected.

   Requesting to detach storage from a virtual machine
   Approval policy that is invoked when detaching storage from a virtual machine. This approval policy suspends the detach storage operation until the generated request is approved or rejected.

   Saving a virtual machine image
   Approval policy that is invoked when saving a virtual machine image. This approval policy suspends the save image operation until the generated request is approved or rejected.

   Requesting to create virtual machine snapshot
   Approval policy that is invoked when creating a virtual machine snapshot. This approval policy suspends the virtual machine snapshot operation until the generated request is approved or rejected.

   Restoring a virtual machine
   Approval policy that is invoked when restoring a saved virtual machine image. This approval policy suspends the restore operation until the generated request is approved or rejected.

   Requesting to revert virtual machine to snapshot
   Approval policy that is invoked when reverting a virtual machine to snapshot version. This approval policy suspends the revert to snapshot operation until the generated request is approved or rejected.

Setting or modifying approval policies for a project

Follow these steps to set or modify an approval policy for a project. These policies override the approval policies that are set for a cloud.

Procedure

1. In the IBM SmartCloud Entry interface, select **Access** > **Projects**.
2. Select the project for which you want to modify approval policies.
3. Select **Customize settings**.
4. Select **Approval Policies**.
5. Set the events that require administrator approval. To use setting defined for a cloud, select **Use cloud default**.

Deploying an image
Approval policy that is invoked when deploying an image to create an instance in the cloud. This approval policy suspends the deployment operation until the generated request is approved or rejected.

Extending the instance expiration time frame
Approval policy that is invoked when extending the expiration date of an existing instance. This approval policy suspends the expiration operation until the generated request is approved or rejected.

Resizing an instance
Approval policy that is invoked when resizing an existing instance. This approval policy suspends the resize operation until the generated request is approved or rejected.

Capturing an instance
Approval policy that is invoked when capturing an existing instance. This approval policy suspends the capturing operation until the generated request is approved or rejected.

Requesting to attach storage to a virtual machine
Approval policy that is invoked when attaching storage to a virtual machine. This approval policy suspends the attach storage operation until the generated request is approved or rejected.

Requesting to detach storage from a virtual machine
Approval policy that is invoked when detaching storage from a virtual machine. This approval policy suspends the detach storage operation until the generated request is approved or rejected.

Saving a virtual machine image
Approval policy that is invoked when saving a virtual machine image. This approval policy suspends the save image operation until the generated request is approved or rejected.

Requesting to create virtual machine snapshot
Approval policy that is invoked when creating a virtual machine snapshot. This approval policy suspends the virtual machine snapshot operation until the generated request is approved or rejected.

Restoring a virtual machine
Approval policy that is invoked when restoring a saved virtual machine image. This approval policy suspends the restore operation until the generated request is approved or rejected.

Requesting to revert virtual machine to snapshot
Approval policy that is invoked when reverting a virtual machine to snapshot version. This approval policy suspends the revert to snapshot operation until the generated request is approved or rejected.

Requests

When deploying an image or when initiating an action that requires approval from an administrator, a request is created and submitted to an administrator for approval. The status is set to Pending until the administrator handles the approval request.

You can set which actions require administrator approval using the Approval policies function. For more information, See “Approval policies” on page 127.

Processing instance requests

When an image is deployed, initiating an instance, the deployment request may require approval by an administrator. The instance status is set to pending until the administrator handles the approval request.

About this task

You can process an instance request from the Instances tab or from the Requests tab. For more information about processing an instance request from the Instances tab, see "Processing requests from the Instances tab" on page 141

To process a pending request, follow these steps:

Procedure

1. In the IBM SmartCloud Entry interface, select **Access** > **Requests**.
2. Expand the **Request Details** section to review or update the request before approving.
3. Expand the **Comments** section to review comments or use the **Add Comment** link to provide additional comments.
   - Click **Approve** to approve the request and allow the deployment processing to start.
   - Click **Reject** to reject the request.
   - Click **Withdraw** to withdraw a request.

Clearing or archiving requests

You can clear or archive requests. Clearing requests deletes the requests while archiving requests saves them to an archive folder. By clearing requests, you can free space on your system and improve performance in the IBM SmartCloud Entry interface. Archive any requests that you may want to reference in the future.

About this task

To clear or archive a request, follow these steps:

Procedure

1. In the IBM SmartCloud Entry interface, select **Access** > **Requests**.
   - To clear requests, click **Clear**.
   - To archive requests, click **Archive**.
2. Use the Request filter to select a subset of requests to clear or archive. Filter by status or start and end date. If you filter by date, you must provide an end date.
   - To clear the selected requests, click **Clear**.
   - To archive the selected requests, click **Archive**. The filtered requests are saved in a file called `requests_<current time in milliseconds>.csv`. This file can be found in the `archives` folder, located in the IBM SmartCloud Entry configuration directory.

Expiration policies

Expiration policies require users to set an expiration period specifying the maximum length of the instance lease and determine the life cycle of expired instances.

You can set a default expiration policy for a cloud or for a project. Expiration policies set for a project override the expiration policies set for a cloud. After an expiration policy has been set, you must set an expiration date whenever deploying an image from that cloud or project. However, the administrative user can set a date with no limitations.

If you are deploying an image from a cloud or project that does not have an expiration policy set, you can choose whether or not to set an expiration date.

The user who deployed the instance will receive an email notification when the instance is about to expire. The user can extend the lease if extensions are enabled.

After the instance expires, it will be stopped. The instance can be automatically deleted after a limited time, specified by the grace period. If no grace period is specified, the instance is deleted immediately. This setting applies whether or not the instance expiration maximum is set.

Updating the default expiration policy for a cloud

You can update the default expiration policy for IBM SmartCloud Entry.

About this task

To update the default expiration policy, complete the following steps:

Procedure

1. In the IBM SmartCloud Entry interface, select **Configuration** > **Clouds**.
2. Click the name of the cloud for which you want to update the expiration policy.
3. Click **Expiration Policies** to open the form.
4. Enter information for the default expiration policy and click **Save**.

   Note: To delete expired instances immediately, set the Grace period to `0`.

Updating the default expiration policy for a project

You can update the default expiration policy for IBM SmartCloud Entry project.

Procedure

1. In the IBM SmartCloud Entry interface, select **Access** > **Projects**.
2. Select a project to open the project update page.

   Note: To delete expired instances immediately, set the Grace period to `0`.
3. Enter information for the default expiration policy.
   - If you select **Use cloud default**, the expiration of the deployment depends on the expiration configuration of the cloud to which the image belongs.
   - If you select **Customize settings**, the expiration policy overrides the expiration policy of the cloud to which images belong.
4. Click **OK**.

Flavors (OpenStack only)

A flavor is the prescribed size of a provisioned virtual machine. Each flavor has a unique combination of resource configurations and sizes.

Updating the flavor for an OpenStack cloud configuration

You can update the flavor that is configured for the cloud.

Procedure

1. In the IBM SmartCloud Entry interface, select **Configuration** > **Clouds**.
2. Select the cloud for which you want to modify flavors.
3. Click **Edit**.
4. Expand the **Flavors** section. You can create a flavor based on an existing flavor or you can create a completely new flavor.

5. Click the flavor name that you want to copy or click the **Create a new flavor** icon to create a new flavor.
6. Set the required values. The required values are **Name**, **Virtual CPUs**, **Memory (MB)**, and **Storage (GB)**.

   Note: When updating the flavor, the processor, memory, and storage size fields only accept integers. Any fractional data is omitted.

Multiple cloud support

IBM SmartCloud Entry allows you to manage multiple clouds from a single instance. For example, you can have a test cloud set up to implement your latest policies before moving those policies to your production cloud.

This support also allows you to manage multiple types of clouds For example, you can have multiple IBM Systems Director VMControl and VMware cloud instances available from a single IBM SmartCloud Entry user interface.

You can customize each cloud to have its own approval and expiration policies as well as configure a network for a specific cloud.

In the Cloud status window, you can see the status of all of the clouds that IBM SmartCloud Entry is connected to. To view details about a specific cloud, select **Cloud settings**.

In the **Clouds** section of the **Configuration** tab, you can add, edit, and delete cloud configurations. When editing cloud configurations, you can also set or update expiration policies and approval policies.

Adding a cloud configuration

You can configure a cloud in the **Clouds** section of the **Configuration** tab.

Procedure

1. Open IBM SmartCloud Entry and select **Configuration** > **Clouds**.
2. Click **Add Cloud**.
3. Enter information in each of the fields that is denoted with a red asterisk (*).

   Note: When you create a VMControl cloud, if the number of virtual machines that you plan to manage with IBM SmartCloud Entry is above 500, it is recommended that the **time out** field be set to 30 minutes to prevent unexpected disconnections between IBM SmartCloud Entry and IBM Systems Director VMControl. The default time out value is 10 minutes. You might use the default and update it from the Cloud update page, as the number of managed instances grows.
4. Click **Add**.

What to do next

After you click **Add**, you are prompted to trust the cloud server SSL certificate. If you do not accept this certificate, the cloud configuration is not added.

Note: If you do not want to accept the default Approval or expiration policies, you can edit the cloud configuration after adding it.

Configuring an OpenStack cloud

After you deploy the IBM SmartCloud Entry Hyper-V appliance, use the web interface to configure an OpenStack cloud.

Procedure

1. Log in to IBM SmartCloud Entry web interface as an administrator.
2. Click the **Configuration** tab and select **Clouds** in the navigation pane.
3. Click the Create a new cloud configuration button.
4. Enter the cloud configuration settings for the OpenStack cloud.

   Name Assign a name to the OpenStack cloud that you want to create.

   Description
   Optionally, add a description for the OpenStack cloud.

   Type Select **OpenStack** for the cloud type.

   Host name
   Select the host name of the appliance or the IP address of the management network (eth0). Selecting **localhost** does not work because the service is listening on the management network.

   Port Accept the default value of **9973**.

   Administrator ID
   Enter *sceagent*, the user ID that is used to communicate between IBM SmartCloud Entry and OpenStack.

   Password
   Type the password for the sceagent user ID. By default it is set to *openstack1*.

   Tenant name
   Type *Public*.

   QPID Settings

   User ID
   Enter *qpidclient*, the user ID that communicates with the QPID messaging server.

   Password
   Type the password for the qpidclient user ID. By default it is set to *openstack1*.
5. Click **Test Connection** to check the current settings.
6. Click **Add** to finish.

Results

If you receive a PKI token error when you are attempting to configure the OpenStack cloud, see “PKI error when adding OpenStack cloud” on page 164 for more information.

OpenStack clouds

When you add an OpenStack cloud, IBM SmartCloud Entry enters a transactional mode for user and project operations. Also, OpenStack relies on Coordinated Universal Time (UTC) time.

When in transactional mode, all user and project operations fail if the OpenStack cloud is unavailable. These operations fail even if the user or project in question is not currently used in connection to OpenStack.

Additionally, IBM SmartCloud Entry uses OpenStack efficient polling with the **changes-since** parameter support to maintain internal caches of certain OpenStack resources. The OpenStack **changes-since** support relies on Coordinated Universal Time (UTC) time to determine if a resource has changed. As a result, the IBM SmartCloud Entry and OpenStack systems must maintain accurate and consistent UTC time to avoid caching and other problems that can occur due to incorrect system time.

Removing a cloud

You can remove an association with a cloud from IBM SmartCloud Entry from the **Clouds** section of the **Configuration** tab.

Procedure

1. Open IBM SmartCloud Entry and select **Configuration** > **Clouds**.
2. Select the cloud that you want to delete.
3. Click **Remove Cloud** and then click **Yes** to confirm.

Results

Note: When removing a cloud configuration, all of the cloud resources created by IBM SmartCloud Entry are lost. Recreating the connection to the cloud at a later time will not recover these resources

Updating a cloud

You can update a cloud in the **Clouds** section of the **Configuration** tab.

Procedure

1. Open IBM SmartCloud Entry and select **Configuration** > **Clouds**.
2. Click the name of the cloud that you want to update.
3. Update the desired fields and click **Save**.

   Tip: From this configuration panel, you can also review or change the **Expiration Policies**, **Approval Policies**, and **Flavors (OpenStack cloud)** of the cloud. For more information, see the following topics:
   - "Expiration policies" on page 130
   - "Approval policies" on page 127
   - "Flavors (OpenStack only)" on page 131

Network configurations

IBM SmartCloud Entry provides a convenient way to manage and apply network settings by using network configurations. Network configurations are a group of network settings for a particular environment, typically a virtual network. These settings can be managed as a single entity and applied to image configurations or instance deployment settings.

For example, suppose that a cloud environment contains two virtual networks applicable to instance deployment: a public and a private virtual network. In this case, an administrator might create two network configurations, one for the public and one for the private. In the public configuration, the administrator would specify all the public network settings such as primary DNS, secondary DNS, and primary gateway. The same would be done for the private network configuration. After the configurations are created, the administrator can configure the images to use the appropriate network configuration. This action saves time by not requiring the administrator to specify each network setting in each image. It also allows an easier way to manage the network settings on a virtual network.

While the actual settings specified in a configuration are tailored to a specific environment, the network configurations themselves are a superset of all network settings regardless of image, operating system, or cloud management system. Therefore, all settings that are specified in a configuration are applicable. For example, the primary and secondary WINS settings of a network configuration are only applicable to Windows based images. So when you create a configuration for an image that is not using Windows, these values are not needed and can be left blank.

Note: With the IBM SmartCloud Entry web interface, you can specify the network configuration for a cloud. The web interface displays only the fields that are applicable for that cloud. Before you can create an OpenStack network configuration, you must select an existing OpenStack cloud.

When network configuration settings are applied to either an image configuration or during an advanced instance deployment, their individual settings can be overridden or manually specified, if wanted.

Note: You cannot override or manually specify OpenStack network configuration settings.

Managing network configurations

You can create, edit, and delete, network configurations from the IBM SmartCloud Entry web interface.

About this task

To create, edit, or delete a network configuration, follow these steps:

Procedure

1. Open IBM SmartCloud Entry and select **Configuration**.
2. Select **Network**.

   The network configurations that are defined in the property files are displayed. The Network tab provides a listing of all existing network configurations, and enables you to edit, create, or delete these network configurations.

   - The Network Configuration column shows the name of the existing network configuration.
   - The Cloud column shows the name of the cloud scope that is associated with the network configuration.
   - The Type column shows the IP address version that the network configuration supports. VMware and VMControl network configurations support only IPv4 addresses, but OpenStack network configurations can support IPv4 or both IPv4 and IPv6 addresses. OpenStack networks do not support IPv6-only addresses.
   - The Available Addresses column shows the number of IP addresses available in the network.
   - The Allocated Addresses column shows the number of IP addresses that are allocated.

   You can edit, create, or delete these network configurations.

   - To view or edit specific network configuration properties, click the network configuration name.
   - To manage the IP addresses for an existing configuration, click **Manage IP Addresses** for the existing configuration.
   - To create a new network configuration, click the New icon.
   - To create a new network configuration that is based on an existing configuration, select a configuration and click the Copy icon.
   - To delete an existing configuration, select a configuration and click the Delete icon.

Adding a network configuration

You can add a network configuration from the IBM SmartCloud Entry web interface.

About this task

To add a network configuration, follow these steps:

Procedure

1. Open IBM SmartCloud Entry and select **Configuration**.
2. Select **Network**.
3. To create a network configuration, click **New**.
4. Specify a cloud scope.

   When you specify a cloud scope, the network configuration that you are adding is only available when you deploy an image to that cloud. If you specify Either VMControl or VMware for the cloud scope, the configuration is available to all VMControl or VMware images. When you specify a cloud scope, this page displays only the fields that are applicable to the selected cloud scope.
5. Enter a name for the configuration.
6. Follow the steps for the cloud scope that you selected.
   - **VMware**
     a. Optionally, enter a description.
     b. Select a unique Network ID.
     c. Select one of the following IP Settings:
        - **Use DHCP**
        - **Use IP address pool**

          If you select **Use IP address pool**, follow these steps:
          1) Specify a Subnet mask and Gateway address. You can also provide an alternative gateway address.
          2) Specify a number of IP addresses and the starting address for allocation. The ending address is calculated based on the number of addresses and starting address.

             Note: If you specify a number of IP addresses, the number must be at least 2. To create a single IP address, you must first create then network configuration, and then add the single IP address.
          3) Specify DNS Settings.
     d. Specify System-wide settings, including Linux and AIX Network Settings and Windows Network Settings.
     e. Choose to be a member of a domain or a workgroup:
        - **Domain**

          If you select Domain, specify the domain name, user, and password.
        - **Workgroup**

          If you select Workgroup, specify the workgroup name.
     f. If you selected **Use IP address pool**, you can also select **Obtain host name and domain name from DNS server**. If you select this option, the DNS used by the system must correlate with the DNS used by this application. If it does not, the names that are obtained might be different from the name that is resolved by the system DNS. If the names cannot be resolved, the host name prefix and domain name that are provided in this configuration are used.
     g. Click **Save**.
   - **VMControl**
     a. Optionally, enter a description.
     b. Select a unique Network ID.
     c. Specify a subnet mask and gateway address.
     d. Specify a number of IP addresses and the starting address for allocation. The ending address is calculated from the number of addresses and starting address.

Note: If you specify a number of IP addresses, the number must be at least 2. To create a single IP address, you must first create then network configuration, and then add the single IP address.

e. Specify DNS settings.

f. Specify System-wide Linux and AIX Network Settings.

g. Specify whether to **Obtain host name and domain name from DNS server**. If you select this option, the DNS used by the system must correlate with the DNS used by this application. If it does not, the names that are obtained might be different from the name that is resolved by the system DNS. If the names cannot be resolved, the host name prefix and domain name that are provided in this configuration are used.

h. Click **Save**.

- **OpenStack**

  a. Select one of the following IP address versions:
  - IPv4 only
  - IPv4 and IPv6

    If you select IPv4 and IPv6, you can enter separate IP address settings for IPv4 and IPv6 addresses. However, the number of IPv6 addresses to allocate must be the same as the number of IPv4 addresses.

  b. Specify a subnet mask (for IPv4) or prefix length (for IPv6) and gateway address.

  c. Specify a number of IP addresses and the starting address for allocation. The ending address is calculated from the number of addresses and the starting address.

  Notes:

  1) There must be at least two IP addresses.

  2) If you attempt to create an OpenStack network with an IP subnet that duplicates or overlaps with an existing OpenStack network, an error message similar to the following is returned:

  ```
  QuantumError: Invalid input for operation: Requested subnet with cidr:
  192.168.0.0/24 for network: 48baeadd-762e-4e47-8007-810a0ae7bee9 overlaps with
  another subnet.
  ```

  The OpenStack network configuration can overlap or duplicate a VMware and VMControl network configuration, but two or more OpenStack network configurations cannot use the same IP address subnet range or overlap. To change this restriction, follow these steps:

  a) Edit `/etc/quantum/quantum.conf` file on the IBM SmartCloud Entry appliance and change the **`allow_overlapping_ips`** property to `True`

  b) Use the sceappmgr tool to restart the OpenStack services.

  d. Specify DNS settings.

  e. Specify provider network settings as follows:
  - Specify one of the following network types:
    - **None selected**

      A network is created based on the **`tenant_network_type`** property in the `/etc/quantum/plugin.ini` file. This value is set to vlan in the SCE image. If this option is used, the physical network name and vlan ID are automatically selected based on the "network_vlan_ranges" property in `/etc/quantum/plugin.ini` file. This property is set to **default:1:4094** in the SCE image.
    - **Flat**

      A virtual network that is realized as packets on a specific physical network that contains no IEEE 802.1Q header. Each physical network can realize at most one flat network.
    - **Local**

A virtual network that allows communication within a host, but not across the network. Local networks are intended mainly for single-node test scenarios.

- **VLAN**

  A virtual network that is realized as packets on a specific physical network that contains IEEE 802.1Q headers with a specific VLAN id. VLAN networks that share a physical network are isolated from each other. Each distinct physical network that supports VLAN networks is treated as a separate VLAN trunk, with a distinct space of VLAN id values.

– If you select **Flat** or **VLAN** for the network type, enter the physical network name.

  This physical network name must match the name that is specified in the **`network_vlan_ranges`** property of the `/etc/quantum/plugin.ini` file.

  Note: You can create only one Flat network on each physical network.

– If you select **VLAN**, enter the VLAN ID.

  Valid VLAN ID values are 1 through 4094.

f. Click **Save**.

Editing network configurations

You can edit a network configuration from the IBM SmartCloud Entry web interface.

About this task

To edit a network configuration, follow these steps:

Procedure

1. Open IBM SmartCloud Entry and select **Configuration**.
2. Click **Network**. The network configurations that are defined in the property files are displayed.
3. Select a network configuration that you want to edit from the list of available configurations. The current properties are displayed for the selected configuration. The properties that are displayed depend on the cloud management system for which the network configuration was created.
4. Click **Edit**. You can edit only certain network configuration properties.
5. Change the properties of the configuration. If you want to edit the IP addresses for this configuration, click **Manage IP Addresses**. For more information about setting up an IP address pool, see “Managing IP address pools.”
6. Click **Save** to save your changes, or **Cancel** to exit the screen without saving your changes.

Managing IP address pools

IBM SmartCloud Entry can automatically select the IP address (or IP addresses) to be used when provisioning a virtual machine from a list of predetermined IP addresses known as an IP address pool. IP addresses are managed and assigned automatically to an instance so that the user requesting the deployment does not need to specify them.

About this task

An IP address is marked as "In Use" when IBM SmartCloud Entry selects that IP addresses from the network configuration and uses it for the deployment of an instance. When the instance is deleted by IBM SmartCloud Entry, the IP address "In Use" indication is cleared so that the IP address can be reused by another instance deployment. If IBM SmartCloud Entry detects that the instance has failed and no longer exists in the cloud, the IP address is unlocked immediately and the "In Use" flag cleared.

The administrator can also mark an IP address or a range of IP addresses as "Locked". "Locked" IP addresses are not selected by IBM SmartCloud Entry for instance deployment. The purpose of "Locked" IP addresses is to allow the administrator to mark certain IP addresses in the network as reserved or "In

Use" by other applications. If the administrator later wants to enable the IP address so that it can be used by IBM SmartCloud Entry for instance deployment, the "Unlock" option can be used to remove the "Locked" indicator.

The main difference between "In Use" and "Locked" is conceptual; addresses that are "In Use" are being used by the IBM SmartCloud Entry application, while addresses that are "Locked" are being used by an external application or are not available as specified by an administrator.

Each network configuration contains its own IP address pool, which allows IP addresses to be managed on a per network configuration basis. If a configuration is applied to the deployment settings of an instance (and the configuration is not set to use DHCP), the IBM SmartCloud Entry automatically uses the pool that is associated with the configuration.

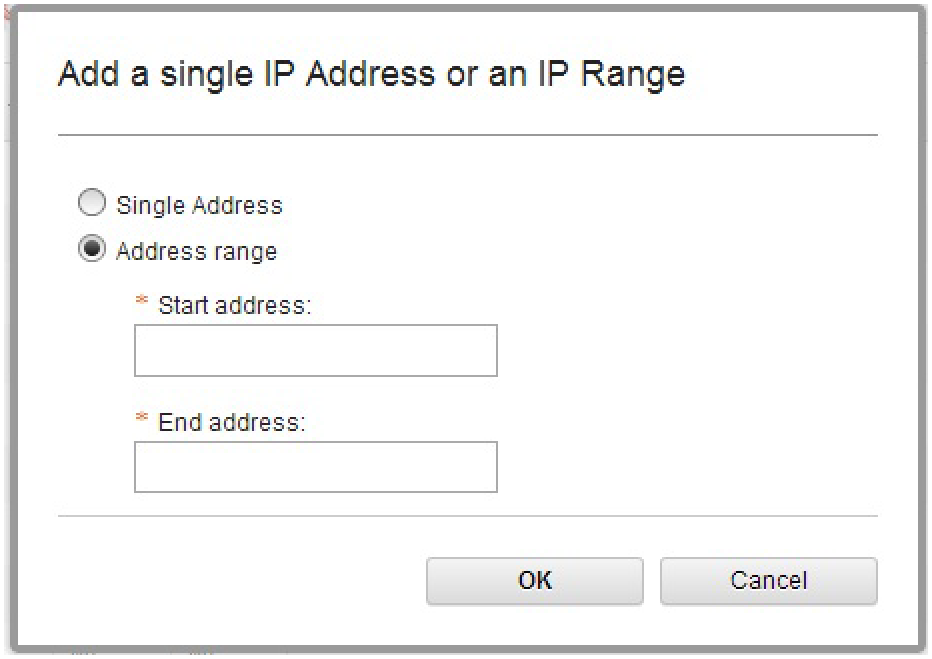
Notes:

1. Network configurations typically represent a VLAN or a virtual network. While a network configuration cannot contain the same IP address more than once, different network configurations can contain the same IP addresses. This behavior was added to allow multiple VLANs to use the same IP address ranges. If the same IP address ranges are specified in multiple network configurations, care must be taken to ensure that these network configurations are used on different networks or VLANs.
2. OpenStack network configurations cannot contain the same IP addresses. Each of the IP subnets that are defined in the OpenStack network configurations must be unique and must not overlap.
3. The IP addresses for an OpenStack network configuration are specified when the OpenStack network configuration is first created. IP addresses cannot be added to or removed from an OpenStack network configuration. Lock and unlock of IP addresses is supported.

The following steps describe how an administrator can manage the IP address pools that are used by the IBM SmartCloud Entry application.

Procedure

1. Open IBM SmartCloud Entry and select **Configuration** > **Network**.
2. From the Network page, select **Edit under IP Addresses**.
3. The **IP Addresses** view is displayed. Use this view to add, remove, lock, or unlock IP addresses.
4. To add IP addresses, select **Add**.
   a. Add an individual or range of IP addresses to the pool.
   b. Select **OK** to add the IP address or range, or select **Cancel** to cancel the operation.



Add a single IP Address or an IP Range

○ Single Address

● Address range

* Start address:

* End address:

5. To remove, lock, or unlock specific IP addresses, select the IP addresses to which to apply the operation, then select **Remove**, **Lock** or **Unlock** from the Manage IP addresses page to apply the operation.

   Note: The IP addresses page allows for smart selection of IP addresses to which to apply the Remove, Lock, and Unlock operations. When Remove, Lock, or Unlock is selected, smart selection determines whether any addresses are selected on the page. If addresses are selected, the operation is applied to the selected addresses without an extra dialog. If no addresses are selected, a dialog is displayed which allows either individual or range based operations for remove, lock, or unlock.

Instances

Use the Instances tab in the IBM SmartCloud Entry interface to manage instances after they have been created.

IBM Systems Director VMControl: An instance in IBM SmartCloud Entry includes metadata about the customization properties used to create the instance and the provisioned virtual server information, unlike a workload in IBM Systems Director VMControl. This metadata is useful for record keeping purposes and provides additional features, such as duplicating instances and instance drafts.

VMware: An instance in IBM SmartCloud Entry is equivalent to a VMware virtual machine. All of the VMware virtual machines are displayed on the IBM SmartCloud Entry Instances tab.

You can filter the list of instances by Cloud, Projects, or Architectures.

As an administrator, you can act on pending instance requests and hide specific instances from appearing to other users.

Note: When starting or restarting IBM SmartCloud Entry on a high scale cloud, the synchronization between IBM SmartCloud Entry and the cloud may take longer than expected. This resynchronization may cause operations such as deploying, deleting, or resizing an instance to be delayed or even fail. Wait for the synchronization to complete before attempting these actions.

Capturing an instance

You can capture an instance or workload to create an image.

For instructions about capturing a workload using IBM Systems Director VMControl, see Capturing a virtual server or workload to create a virtual appliance in the IBM Systems Director information center at http://pic.dhe.ibm.com/infocenter/director/pubs/topic/com.ibm.director.vim.helps.doc/fsd0_vim_t_capturing_workloads.html.

Note: On a KVM system, you can capture only instances that are stopped.

For information about capturing an OpenStack instance, see “Considerations for capturing an OpenStack instance” on page 103

Pinning an instance

In a deployed instance, you can pin a virtual machine to a specific physical host to prevent the server from being relocated. However, an instance or workload that is set to be highly available cannot have pinned virtual machines.

Procedure

1. In the IBM SmartCloud Entry interface, select **Instances**.
2. Select an instance to open the properties.
   - To pin an instance, select **Pin**.
   - To unpin an instance, select **Unpin**.
3. Click **Close**.

Processing requests from the Instances tab

When an image is deployed, initiating an instance, the deployment request may require approval by an administrator. In this case, the instance status is set to pending until the administrator handles the approval request.

About this task

You can process an instance request from the Instances tab or from the Requests tab. For more information about processing an instance request from the Requests tab, see “Processing instance requests” on page 129

To process a pending request, follow these steps:

Procedure

1. In the IBM SmartCloud Entry interface, select **Instances**.
2. Select an instance name to view the instance details. Find the request list in the instance details and select a request to display. The Request properties page appears.
3. Expand the **Request Details** section to review or update the request before approving.
4. Expand the **Comments** section to review comments or use the **Add Comment** link to provide additional comments.
   - Click **Approve** to approve the request and allow the deployment processing to start.
   - Click **Reject** to reject the request.
   - Click **Withdraw** to withdraw a request.

Hiding or showing an instance

Follow these steps to show or hide an instance.

Procedure

1. In the IBM SmartCloud Entry interface, select **Instances**.
2. Select an instance and click **Hide/Show** to hide or show the instance in the instance list for all non-administrative users.
3. After an instance is hidden, a non-administrative user does not see the instance in the instance list, but administrative users can choose to display the hidden instance. To display hidden instances in the instance list, select **Include hidden instances**.

Resizing an instance (VMControl)

You can modify the amount of resources that are used by the virtual machines.

Before you begin

If your instance is running on a KVM, make sure that the instance is stopped before you continue the procedure.

Procedure

1. Click the name of the instance that you want to resize.
2. Click **More** > **Resize...** to open the Resizing instance page.
3. Update the number of processors, processing units, and memory resources to be allocated to the virtual machine in your instance.
4. Click **Resize**.

   Tip: If you see zeros in the fields you updated, it can take up to two hours for the updated values to be reflected.

   Note: If approvals are enabled, then the approval must be completed before the instance is resized.

Resizing an instance (VMware)

You can modify the amount of resources used by the virtual machines provisioned by your instance running on VMware. Depending on how your VMware virtual machines are configured, you can add memory and virtual processors while your virtual machine is running.

About this task

Increasing the size of the virtual machine disks makes more space available on the disk, but does not change the size of the partitions and the file systems. There are commands that must be run on the guest operating system to increase the size of the file system. For more information about how to change the size of the file system after storage is added, see your operating system documentation.

For more information about how a running virtual machine handles changes in memory and processor, see the VMware documentation and your operating system documentation.

Procedure

1. Click the name of the instance that you want to resize.
2. Click **More** > **Resize**.
3. Update the number of processors and memory resources to be allocated to the virtual machine in your instance.

   The settings that can be resized when a virtual machine is in the started state depend on how the virtual machine is configured on VMware:

Note: If the instance is started and the virtual machine is not configured to allow memory or processor changes, those fields are not displayed. To change those values, you must first stop the instance.

- For memory, the virtual machine must have the Memory Hot Add option enabled. Memory is only allowed to be increased, and the maximum amount allowed, and the valid values, are determined by VMware.
- For processors, the virtual machine must have the CPU Hot Plug option enabled. To remove processors, the virtual machine must have the CPU Hot Add and Remove option enabled. The maximum number of processors allowed is determined by the number of logical processors on the vSphere machine that is running the virtual machine.

4. Increase the disk size.
5. Click **Resize**.

   Note:

   - If approvals are enabled, then the approval must be completed before the instance is resized.
   - Linked clone disks or disks that are using an IDE controller cannot be resized.

Resizing an instance (OpenStack)

You can modify the amount of resources that are used by the virtual machines.

About this task

Stop the instance before you continue the procedure.

Procedure

1. Click the name of the instance that you want to resize.
2. Click **More** > **Resize...** to open the Resizing instance page.
3. Under the **Hardware** section, update the **OpenStack Flavor** to be allocated to the virtual machine in your instance.

   Note:

   - The flavor details change depending on the size flavor that you select.
   - When you update the flavor, the processor, memory, and storage size fields accept integers only. Any fractional data is omitted.
   - If you are changing the storage size, you can update to a larger disk size only.
4. Click **Resize**.

   Note: If approvals are enabled, then the approval must be completed before the instance is resized.

   If you are resizing an instance on the Hyper-V hypervisor, the **`IBMComputeNodeService`** service that is deployed with the Hyper-V agent installer must run with domain credentials and configure Kerberos constrained delegation. You can set the service credentials with: `C:\sc config "IBM SmartCloud Entry Compute Service" obj="DOMAIN\username" password="password"`.

   To configure the Kerberos constrained delegation setting, see step 1 in the following guide: Configure constrained delegation.

Users

The **Users** tab in the IBM SmartCloud Entry is enabled for administrative users and is used for creating, viewing, and managing users.

Creating a user

Complete the following steps to create a user.

Procedure

1. In the IBM SmartCloud Entry interface, select **Access**.
2. Select **Users**.
3. Click **New User**.
4. Enter information for the new user.
5. Click **Create**.

   Note: You can only create valid user accounts when using local authentication. When using LDAP authentication, user accounts are created and managed directly through the LDAP server.

Viewing or updating a user

About this task

To view or update information about a user, follow these steps:

Procedure

1. In the IBM SmartCloud Entry interface, select **Access**.
2. Select **Users**.
3. To view or update information about a user, select the user you want to view.

Unlocking a user

If a user has three invalid login attempts in a 24 hour period, the user account becomes locked and requires an administrator to unlock it.

About this task

To unlock a user, follow these steps:

Procedure

1. Open IBM SmartCloud Entry and select **Access**.
2. Select **Users**.
3. Select the user to unlock and click **Unlock Users**.

Deleting a user

Complete the following steps to delete a user.

Procedure

1. In the IBM SmartCloud Entry interface, select **Access**.
2. Select **Users**.
3. Select the user you want to delete from the list of users and click **Delete**.
4. To confirm the user deletion, select **Yes**. To cancel the user deletion, select **No**.

User management with OpenStack

Unlike other cloud types, OpenStack clouds provide native support for user management through the OpenStack keystone component.

When you first connect to an OpenStack cloud, IBM SmartCloud Entry imports all the user accounts that currently exist in OpenStack. All user roles and project membership are accepted and reflected in IBM SmartCloud Entry.

After IBM SmartCloud Entry imports the initial OpenStack users and connects to an OpenStack cloud, IBM SmartCloud Entry enters transactional mode for user management. When in transactional mode, all operations that are performed in IBM SmartCloud Entry are also performed in OpenStack (for example, keystone). If a user management operation (such as any of the operations that are described in this section) fails to complete successfully in IBM SmartCloud Entry, it does not occur in OpenStack. Likewise, if it fails in OpenStack it reverts in IBM SmartCloud Entry.

IBM SmartCloud Entry enters transactional mode for user operations while connected to OpenStack so that the user registries in both products are always synchronized. For this reason, when connected to an OpenStack cloud, it is not possible to perform user-related operations while the OpenStack cloud is down or unavailable.

To connect to OpenStack, IBM SmartCloud Entry uses a service user account and a default service tenant. Some installations of OpenStack have user accounts specific to OpenStack components (for example, nova, keystone, quantum). These and other service user accounts or service tenants in an OpenStack server that do not represent an actual user account or tenant, can be added to the list of service users and service tenants so that they are ignored by IBM SmartCloud Entry. To make this change, add the service users and tenants to the comma-separated list of users in the *com.ibm.cfs.cloud.openstack.service.users* property, or the comma-separated list of tenants in the *com.ibm.cfs.cloud.openstack.service.tenants* property, in the *openstack.properties* file.

Accounts

You can view information for those accounts of which you are either an owner or a member.

Accounts are required when IBM SmartCloud Entry billing is enabled. Guidelines for IBM SmartCloud Entry billing are:

- Only IBM SmartCloud Entry administrators can create accounts, but you can be made an account owner.
- You can deploy instances only if you are an account member and the account has a positive balance with which to pay for server use.
- Only account owners and IBM SmartCloud Entry administrators can manage accounts.
- Accounts have a balance, an owner, an account balance threshold, account members, and invoices.
  - The *balance* is a monetary balance of the account. The cost of each request and running deployment is subtracted from the balance over time.
  - The account *owner* is the IBM SmartCloud Entry user profile that is accountable for crediting and paying the account.
  - The *account balance threshold* is a value that represents the amount at which the account balance becomes a *low balance*. If the balance drops to zero, the account is delinquent.
  - The *account members* are IBM SmartCloud Entry users that belong to the account. When account members deploy instances in IBM SmartCloud Entry, the instances are billed to their account.
  - Each instance has an *invoice*. An account can have many invoices which are viewable from the Account properties window.

Creating an account

You can create an account at any time.

Procedure

1. Click **New Account**.

2. Enter information for the new account. Both the **Account name** field and the **Account owner** field are required.
3. Click **Create.**

Add members to an account

You can add members to your account at any time, however, users can only be members of one account at a time.

Procedure

1. In the account table, select the account to which you want to add members.
2. To open the account member management window, click **Edit list**.
3. To add a member, select the member to be added from the **Available users** list and click **Add**.

Viewing or managing an account

You can view the properties of any account, or manage the accounts that you own.

About this task

To view account properties or manage accounts that you own, select the **Access** tab and click **Accounts**. Then, you can select the account that you want to work with in the account table.

Deleting an account

You can delete an account only if you are the owner of the account, and only when the account is not associated with any active instances.

Procedure

1. In the account table, select the account you want to delete.
2. Click the **Delete** icon and confirm the deletion.

Clearing or archiving events

From the Events tab, you can see events such as instance completion, instance failure, new account requests, and new accounts created. You can also clear or archive events. Clearing an event deletes it while archiving an event saves it to an archive folder. By clearing events, you can free space on your system and improve performance in the IBM SmartCloud Entry interface. Archive any events that you may want to reference in the future.

About this task

To clear or archive an event, follow these steps:

Procedure

1. In the IBM SmartCloud Entry interface, select **Reports** > **Events**.
   - To clear an event, click **Clear**.
   - To archive an event, click **Archive**.
2. Use the Events filter to select a subset of events to clear or archive. Filter by severity or start and end date. If you filter by date, you must provide an end date.
   - To clear the selected events, click **Clear**.
   - To archive the selected events, click **Archive**. The archived events are saved to a file called `events_<current time in milliseconds>.csv`. This file is can be found in the `archives` folder, located in the IBM SmartCloud Entry configuration directory.

Chapter 14. Security

IBM SmartCloud Entry offers security options such as secure sockets layer (SSL), Lightweight Directory Access Protocol (LDAP), and user administration. This section provides information on managing passwords that are associated with the security options.

Passwords

The following list provides links to various sections in this document that describe default passwords and places where passwords are entered and stored in IBM SmartCloud Entry.

- Chapter 6, “Installing IBM SmartCloud Entry,” on page 23
- “IBM SmartCloud Entry for Cloud SSL configuration (optional)” on page 31
- “Deploying the Hyper-V virtual appliance” on page 47
- “Deploying the KVM virtual appliance” on page 52
- “Deploying the VMware virtual appliance” on page 53
- “Managing passwords” on page 57
- “Starting, stopping, and status of the IBM SmartCloud Entry application on IBM SmartCloud Entry for System x virtual appliance” on page 58
- Chapter 11, “Installing the IBM SmartCloud Entry Hyper-V Agent,” on page 63
- “Configuring REST API authentication” on page 81
- “Configuring database” on page 82
- “Configuring global image deployment” on page 84
- Set secure access during deployment (Linux on VMware)
- “Creating a configuration strategy” on page 98
- “Configuring the default administrator user account” on page 115
- “Configuring LDAP authentication using the web interface” on page 115
- “Adding a network configuration” on page 135

Chapter 15. Best practices for using IBM SmartCloud Entry

Back up and restore IBM SmartCloud Entry

To protect your IBM SmartCloud Entry data, you must back up critical files in case the server enters an undesired state. Before you back up your data, determine the circumstances in which you intend to restore your data.

Backing up server data for recovery

There are two kinds of data to back up. The first set of data is for server configuration and the second set of data is used by the database. When you consider what data to back up, review both sets of data.

Note: This procedure backs up IBM SmartCloud Entry only. It does not back up the underlying virtualization managers, such as VMware vCenter or storage devices.

1. Stop the IBM SmartCloud Entry server to ensure that the backup data is complete.
2. Back up the following configuration files.
   - The `.SCE31` folder.
   - In the `installation` folder: `skc.ini`

     Note: If any values are changed in this file, you must back up the updated file after you change default values.

A copy of all these files is required to ensure a complete backup.

Backing up database data for recovery

All of the database data that is related to IBM SmartCloud Entry users, such as projects, networks, instances, images, are stored in the database. The backup procedure is different depending on the database that is being used.

1. Stop the IBM SmartCloud Entry server to ensure that the backup data is complete.
2. Follow the instructions that pertain to your specific database.

   Derby database

   If you are using the Derby database, backup the `.SCE31/database folder` that stores all the database data.

   DB2 database

   If DB2 is configured, backup the database in the DB2 server. For more information about how to back up the DB2 server, see the DB2 Information Center.

   Note: Ensure that the information referenced matches the version of DB2 that you are using. If not, reference the appropriate support documentation for similar information.

Restoring the server

To restore a backup of the server and the Derby database, copy all the saved files back to the original server. After the copy is complete, start the IBM SmartCloud Entry server.

If you are using the DB2 database, there are some extra steps.

1. Ensure the path that is specified in the `database.properties` configuration file, by the property *database.db2.path*, is correct.

```
# If db2 then the path to the DB2 dtatbase needs to be provided. This will be ignored for derby.
#database.db2.path=//localhost:50000/cfs:.
```

Essentially, creating a backup of the entire `home` folder and `skc.ini` file ensures a complete backup of the IBM SmartCloud Entry server. Copying the files back to their original location restores the data.

Considerations for backing up a IBM SmartCloud Entry appliance

To back up a IBM SmartCloud Entry appliance, use the existing snapshot or capture capabilities that are provided by the underlying virtualization manager. First, ensure that all services are turned off before you attempt to take a snapshot of either Hyper-V or VMware. If you are using KVM, the process depends on your existing infrastructure. For example, if SAN storage is being used, use the FlashCopy® function to take a snapshot of the appliance disks.

Important: There is a limitation to be aware of when you use this best practice. Any incremental data that occurs after backing up the IBM SmartCloud Entry server is lost after you restore the server. Therefore, some functions might not work as expected. For example, consider the circumstance where you create an instance after you complete a capture, and then you restore the server. The IP address that was assigned to the instance (after the backing up) is still available in the IP address pool. It might be assigned to another instance.

Using the `screen` command

The **`screen`** command can be used to start or shut down the IBM SmartCloud Entry server or to access the OSGI console when the server is up and running when running Linux.

For example, enter **`screen`** and then run the command to start the server. After the server is started, type `ctrl+a`, then `d` to disconnect and leave the IBM SmartCloud Entry server running,

To get back to the IBM SmartCloud Entry OSGI prompt to perform other actions, such as enabling additional logging, enter `screen -r`.

Using the `nohup` command

On AIX or Linux, if you start a process from the command line and then log off, the processes you started are generally terminated, even if you spawn them as background processes, because each process is sent a hang up signal (`SIGHUP`). The **`nohup`** command allows you to start a process with the hang up signal disabled so that the process is not ended when you log off.

The **`nohup`** command is used frequently for starting services, such as ssh daemon or DB2 instances.

For example, to start IBM SmartCloud Entry as a background service, run the following command:

```
nohup /opt/ibm/SCE24/skc -nosplash < /dev/null > /dev/null &
```

The options in this command include the following:

-nosplash
Prevents the process from displaying a splash screen.

< /dev/null
Disconnects the process from terminal input. This option can prevent the process from entering a *stopped* state as can sometimes happen when started from the command line on AIX. This option is not needed when starting the command from a shell script.

> /dev/null
Redirects the OSGI console output. For example, you might want to redirect the output to a log file.

& Runs the command as a background process.

Deploying 500 virtual servers to a VMControl cloud in a 24 hour period

If you plan to deploy more than 500 virtual servers to an IBM Systems Director VMControl cloud in IBM SmartCloud Entry within a 24 hour period, you must update the `deployment.properties` file in the home directory.

Complete the following steps to update the `deployment.properties` file so that only one **`lscustomization`** call is completed during the deployment request.

1. Locate the `deployment.properties` file for IBM SmartCloud Entry. By default, the `deployment.properties` file is in the `/root/.SCE31/deployment.properties` path.
2. Edit the `deployment.properties` file so that the **`com.ibm.cfs.deployment.static.appliance.customization`** setting is `true`. See the following example:

```
#True to use the set of static customization properties that are configured for an appliance. The only
#way to get updated properties from the cloud when this is true is for the administrator to configure
#the appliance. Note that the static properties are stored in the locale of the initial requester
#which may not match the current user. When this is false, the default, the customization properties
#are retrieved from the cloud on each deployment.

com.ibm.cfs.deployment.static.appliance.customization=true
```

3. After you make the update to the **`com.ibm.cfs.deployment.static.appliance.customization`** setting, restart IBM SmartCloud Entry to enable the setting.

Chapter 16. IBM SmartCloud Entry for System X

IBM SmartCloud Entry for System X is installed as a pre-integrated software stack, and delivered as virtual images that automate IT service deployment in a virtual environment.

IBM SmartCloud Entry version 3.1 provides images for Linux Kernel-based Virtual Machine (KVM) /IBM Systems Director VMControl, VMware vCenter, and Hyper-V.

IBM SmartCloud Entry simplifies the process of common public or private cloud operations, such as:

- Provisioning and de-provisioning virtual machines
- Capturing an instance to create a new virtual image
- Starting up and shutting down virtual machines
- Resizing existing virtual machines
- Creating projects to give team-specific access to instances
- Providing network configurations, which set unique network properties to different instances
- Billing, accounting, and metering support
- Providing request and approval instance support

If you are using Tivoli Provisioning Manager for Images, see your product documentation for more information about management capabilities.

IBM Systems Director Standard Edition

You can install IBM Systems Director to provide system management and health reporting.

For more information about IBM Systems Director, see the Installing IBM Systems Director Standard Edition for IBM x86 topic.

Tivoli Provisioning Manager for Images

With Tivoli Provisioning Manager for Images, you can capture an existing instance to deploy a new image.

The primary use of Tivoli Provisioning Manager for Images within IBM SmartCloud Entry is to create a deployable image from an existing instance. The following steps are required to complete this task:

1. Create the boot media.
2. Capture the virtual image.
3. Deploy the virtual image.
4. Convert the VMware virtual image to a IBM SmartCloud Entry image.

For more information about Tivoli Provisioning Manager for Images, see the IBM Tivoli Provisioning Manager for Images Information Center.

For information about automating and simplifying physical to virtual machine conversions, see the VMware vCenter Converter Documentation.

Chapter 17. Troubleshooting

This section describes various suggestions and references to information that may be helpful when troubleshooting problems and issues with IBM SmartCloud Entry.

IBM SmartCloud Entry FAQ

The frequently asked questions (FAQ) topic is a list of questions and answers about IBM SmartCloud Entry.

Q: **How do I find my home directory?**

A:

1. In Windows, enter `% HOMEPATH%` in the address bar of a Windows Explorer window
2. In AIX or Linux, type `echo $HOME` in a command window.

Q: **I created a trusted certificate. Why am I still getting an exception that says the connection is untrusted?**

A: When the CA is not trusted by clients automatically and you are attempting to access IBM SmartCloud Entry with the https protocol, an exception is encountered that says the connection is untrusted. You must confirm that the risks are understood and must add an exception to continue. Even with a trusted certificate, when you are using Internet Explorer, a similar exception is likely to occur.

Q: **I want to have spaces in my directory name, but it keeps failing when I try to create it. How can I have spaces?**

A: If you have spaces in a directory name, then you must have double quotation marks around it as shown in the following example: `sce240_windows_installer.exe -i silent -f "c:\My Directory\installer.properties"`

Q: **My user ID is locked! How do I unlock it?**

A: If you have three invalid attempts to log in to IBM SmartCloud Entry in a 24 hour period, your user ID is locked and must be unlocked by an administrator. If your administrator ID becomes locked, you can either wait 24 hours without logging in or restart IBM SmartCloud Entry and then try logging in again.

Q: **IBM SmartCloud Entry GUI looks distorted. How can I fix that?**

A: See the information in "Display issue with Internet Explorer" on page 159.

Q: **I upgraded/installed IBM SmartCloud Entry version 2.4, but I'm still seeing the previous version in my browser. How can I fix that?**

A: Clear the cache in your browser and try again. You might have to close your browser after you clear the cache and then reopen your browser and try connecting to IBM SmartCloud Entry version 2.4 again.

Q: **My image is not visible in the window. Where is it?**

A: Make sure that your image is deployed and that the correct project is specified. If it still is not visible, contact the administrator to ensure that you have access.

Q: **The product charges that I set are incorrect or are not updating. What do I do?**

A: First of all, verify that the currencies for all configurable products are the same. You cannot mix currencies. To change your currency for a product, see the "Configuring billing" on page 107. Make sure that you are restarting IBM SmartCloud Entry after saving.

Q: **The instances for a user were moved to a different project. Now when the user logs on, he cannot see his instances. How can the user access his instances?**

A: The project where the instances were moved might need to be edited to grant the user access to the project. When you have ensured that the user has access to the new project, have the user check again to see whether the instances display.

Q: **IBM SmartCloud Entry will not start for me. I am running Windows. Why am I having problems?**

A: You must be the Windows Administrator to run IBM SmartCloud Entry. However, if you are in the administrator group, you can right-click the IBM SmartCloud Entry icon and select **Run as Administrator**.

Q: **When updating IBM SmartCloud Entry to a new release, can I migrate data and configurations from two releases previous to the current release? For example, can I migrate data in IBM SmartCloud Entry from version 2.2 to version 2.4?**

A: No, you must migrate sequentially. For example, migrate from IBM SmartCloud Entry version 2.2 to version 2.3. Then you can migrate from IBM SmartCloud Entry version 2.3 to version 2.4.

Q: **Does the IBM SmartCloud Entry infocollect command support collecting a database log such as DB2?**

A: No, you must check with the administrator of the database and collect the log manually.

Q: **Why does my login fail with the session timing out?**

A: If your user login fails because the session times out, there might be a problem with the timezone setting. Verify that the IBM SmartCloud Entry server and client time and timezone match. For example, on the server, if the timezone is Coordinated Universal Time +08:00, the time is 11:27. For the client, the timezone is Coordinated Universal Time +07:00, and the time should be 10:27.

Logging tasks

The IBM SmartCloud Entry log files are a source of information for additional details about IBM SmartCloud Entry errors.

By default, IBM SmartCloud Entry creates a log file in the `<home directory>/logs` directory and saves 9 log files of 50 MB each. The latest log file is called `skc-0.log`.

Change logging levels from the OSGi command prompt

The logging levels can be changed dynamically while the server is running by using the **`log`** command from the IBM SmartCloud Entry (OSGi) command prompt.

About this task

The logging levels can be changed dynamically while the server is running by using the **`log`** command from the IBM SmartCloud Entry (OSGi) command prompt. Changes made using the **`log`** command are not saved and are only in effect while the server is running. If the server is restarted, the logging levels are reset to their initial values as specified in the `logging.properties` file. For more information about changing these values in the `logging.properties` file, see "Configuring logging" on page 105.

To run the **`log`** command, follow these steps:

Procedure

1. Access the IBM SmartCloud Entry OSGi console.
2. At the OSGi command prompt enter `log <action> <action parameters>`, where the following actions are supported:

   help Displays the online help.

list Lists the available loggers and their current levels.

setlevel <logger name>=<logger level>
Sets the specified logger to the specified logging levels. To set more than one logger, separate the logger name=logger level pair with a space.

Results

See the following examples for typical log commands:

```
log help
log list
log setlevel com.ibm.cfs.cloud=finest
log setlevel com.ibm.cfs.cloud=info default=finest
```

The most common log message level that an IBM SmartCloud Entry administrator might want to change is `com.ibm.cfs.rest.client.internal=FINE`. Changing the message level causes the output of HTTP requests and responses to be sent to and from the VMControl REST API.

In a production environment, keep a backup of the log files for at least two weeks to help resolve problems that are not reported immediately or that go undetected.

Note: The property file values are not case-sensitive so a property such as `com.ibm.cfs.rest.client.internal=FINE` is the same as `com.ibm.cfs.rest.client.internal=fine`.

Retrieve log and system files

IBM SmartCloud Entry provides a command-line utility that enables you to gather logs and system information. If you are using the packaged IBM SmartCloud Entry appliance and the OpenStack cloud, then standard OpenStack logs can also be collected. When you use standard OpenStack logs you do not have to use *log_config* to customize the configuration. This tool runs independently of IBM SmartCloud Entry and is available even when IBM SmartCloud Entry is not running.

To use the command-line utility, run one of the following commands:

- **`infocollect.bat`**: on a Windows system.
- **`infocollect.sh`**: on Linux or AIX systems

Note: These scripts can be found in the `SCE_INSTALLATION_DIR/bin` directory.

The command accepts the following options:

-c Specifies the configuration directory, for example: `SCE_HOME`, where all the IBM SmartCloud Entry configuration and log files are saved. If this argument is used, provide an existing directory path. If this argument is not provided, the command uses `USER_HOME/.SCE31` as default. The command exits with an error if the default `USER_HOME/.SCE31` or the specified directory cannot be found.

-d Specifies the destination directory for the result files. If this argument is used, provide an existing directory path. This command exists with an error if the specified. If this argument is not provided, the `HOME` directory of the caller is used. If the `HOME` directory is not found, for example, the corresponding environment variable is not set correctly, the system `TEMP` directory is used as the default output directory. For example, in Linux `/tmp` is the system `TEMP` directory and in Windows 7, the `%USER_HOME%\AppData\Local\Temp` is the `TEMP` directory.

-h Prints usage information.

When this utility is invoked, the following files are created:

`openStackLog.zip(Optional)`
Contains all of the OpenStack log files:

`*.log` files

*.gz files

sceHome.zip

Contains all of the IBM SmartCloud Entry configurations:

*.properties files

*.log files

*.udr files

Billing configurations: .xml files under products/

All .xml and .txt files under SCE_HOME

basicSysInfo.txt

Contains basic OS information:

CPU

Memory

OS name

Note: This information is retrieved by calling OS shell commands (for example, **DOS** commands for Windows), so the results vary depending on the concrete OS.

Example 1

Collect the configurations, logs, and system information, and save the result to the F:\documents\sce\diagnostic directory. The SCE_HOME is C:\Users\Admin\.skc. If the C:\Users\Admin is the home directory of current user, the -c argument can be ignored.

```
infocollect.bat -c C:\Users\Admin\.SCE24 -d F:\documents\sce\diagnostic
```

Example 2

Collect the configurations in Linux or AIX, logs, and system information, and save the result to the directory of /home/sceAdmin/documents/sce/diagnostic. The SCE_HOME is /home/sceAdmin/.skc. If the /home/sceAdmin is the home directory of current user, the -c argument can be ignored.

```
infocollect.bat -c /home/sceAdmin/.SCE24 -d /home/sceAdmin/documents/sce/diagnostic
```

Troubleshooting using the OSGi console

Use the Open Services Gateway initiative (OSGi) console to review information about IBM SmartCloud Entry.

By default, IBM SmartCloud Entry starts an OSGi command-line console when the IBM SmartCloud Entry executable is run. You can access the console directly in the command window started by the executable.

You can also run the console in the background and assign a specific port for telnet connections. To assign a port, modify the skc.ini file and add an unused port number on a new line after the -console option.

```
-console
<port number>
```

For example, to assign port 7777 for telnet connections, change the option to the following:

```
-console
7777
```

To connect to the OSGi console, type the following:

```
telnet localhost 7777
```

Known issues

Two users within the same browser

Logging in as two different users within the same browser shows only the most recent user.

Details

Different tabs or windows of the same browser instance share the same session and browser cookies so the user does not really have two independent sessions. If a user logs in with two different user IDs at the same time, the browser will use information based on that most recent login, and there is no clear indication that one just superseded the other. For example, if a user logs in as UserA in one browser window and UserB in another browser window, both windows are UserB, and all content and settings displayed belong to UserB.

Solution

To log in as a different user with a browser, log out and close all browser instances before logging in as the alternate user. To log in as two different users at the same time, two different browsers are needed, for example, Internet Explorer and Mozilla Firefox.

Display issue with Internet Explorer

IBM SmartCloud Entry layout and format sometimes appear to be out of place and hard to navigate in Internet Explorer 9 and Internet Explorer 10.

Details

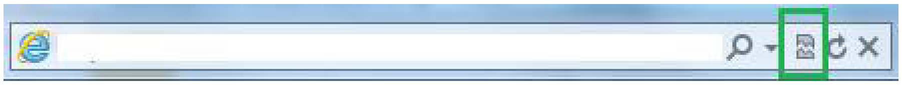
When you are using IBM SmartCloud Entry in Internet Explorer 9 and Internet Explorer 10, you might experience that the layout and format of the screen is difficult to navigate.

Solution

The display issue occurs because Internet Explorer 9 and Internet Explorer 10, by default, display IBM SmartCloud Entry in Internet Explorer Compatibility View mode. To resolve this issue, you must switch from Internet Explorer Compatibility View mode to the standard mode.

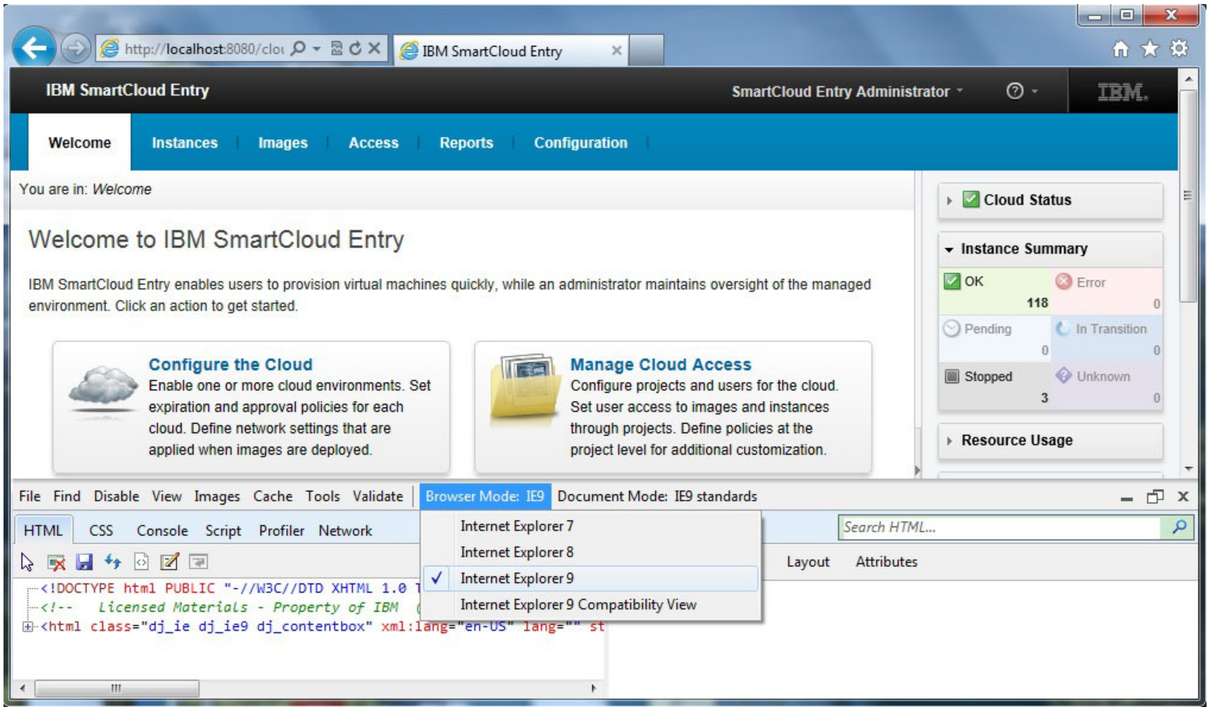
1. To switch from Internet Explorer Compatibility View mode to the standard Internet Explorer mode, click **Compatibility View**.

   The **Compatibility View** icon is found to the right of the address bar.

2. If the **Compatibility View** icon is not visible, press **F12**.
3. Depending on which version of Internet Explorer you are using, continue with one of the following steps:
   - If you are using Internet Explorer 9, click **Browser Mode: IE9 > Internet Explorer 9** to select the standard mode.

Note: The only check mark in the menu is in front of Internet Explorer 9.



You are in: *Welcome*

Welcome to IBM SmartCloud Entry

IBM SmartCloud Entry enables users to provision virtual machines quickly, while an administrator maintains oversight of the managed environment. Click an action to get started.

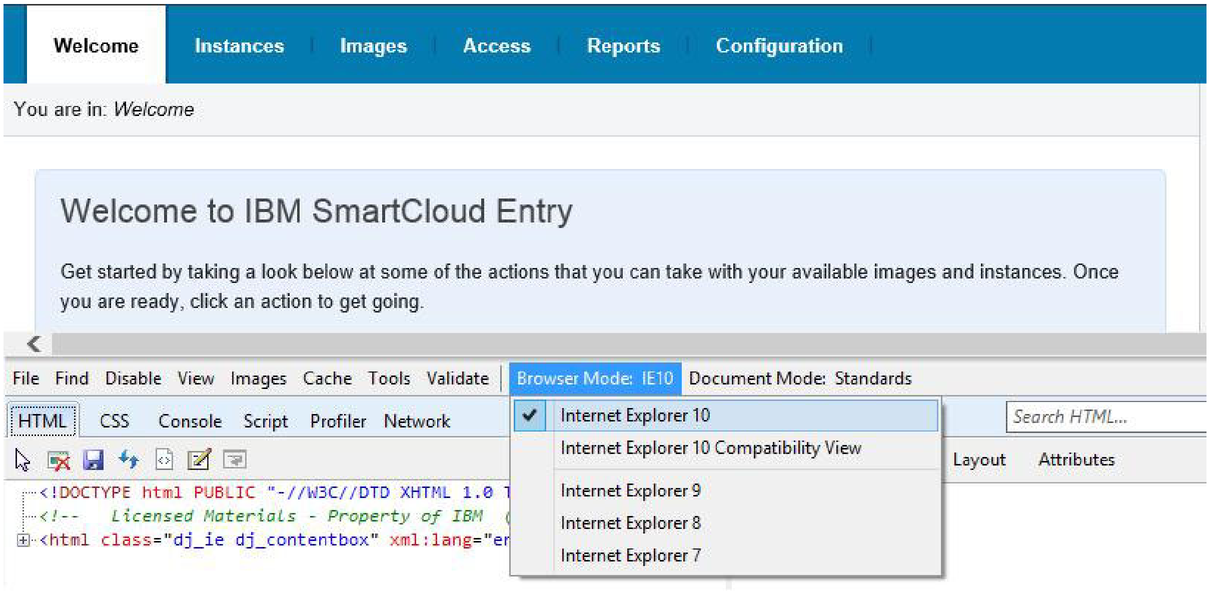
Configure the Cloud
Enable one or more cloud environments. Set expiration and approval policies for each cloud. Define network settings that are applied when images are deployed.

Manage Cloud Access
Configure projects and users for the cloud. Set user access to images and instances through projects. Define policies at the project level for additional customization.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 T
<!--   Licensed Materials - Property of IBM   (
<html class="dj_ie dj_ie9 dj_contentbox" xml:lang="en-US" lang="" st
```

- If you are using Internet Explorer 10, click **Browser Mode: IE10 > Internet Explorer 10** to select the standard mode.

  Note: The only check mark in the menu is in front of Internet Explorer 10.



You are in: *Welcome*

Welcome to IBM SmartCloud Entry

Get started by taking a look below at some of the actions that you can take with your available images and instances. Once you are ready, click an action to get going.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 T
<!--   Licensed Materials - Property of IBM   (
<html class="dj_ie dj_contentbox" xml:lang="er
```

Tip: If IBM SmartCloud Entry switches from standard mode to compatibility view mode automatically, clear the option in **Tools** > **Internet options** > **Advanced** > **Automatically recover from page layout errors with Compatibility View**.

No billing information for processor and memory products

With billing enabled in IBM SmartCloud Entry using a VMControl Cloud, the product entries for processor and memory are not appearing on the bill; only the disk information shows up.

Details

When enabling the billing capabilities in the IBM SmartCloud Entry with a VMControl Cloud, currently the products marked as CPU and RAM defined in the /product directory in the home directory, are not recognized.

Solution

In order to get them recognized by the framework, you must change the product ID in those XML files from the original to a new ID. For example, the CPU XML product file is similar to the following:

```
<cloudProduct id="com.ibm.cfs.services.billing.products.cpu">
 <name>CPU</name>
 <description>The amount of CPUs used in a Deployment per hour.</description>
 <!-- $0.0167 per minute = ~$1.00 an hour. Per processor. -->
 <pricing currency="USD" interval="10" price="0.167"/>
 <collector property="Processor.Reservation"/>
</cloudProduct>
```

The line <cloudProduct id="com.ibm.cfs.services.billing.products.cpu">, needs to have the ID changed to a different ID, similar to the following:

```
<cloudProduct id="com.ibm.cfs.services.billing.products.cpu2">
 <name>CPU</name>
 <description>The amount of CPUs used in a Deployment per hour.</description>
 <!-- $0.0167 per minute = ~$1.00 an hour. Per processor. -->
 <pricing currency="USD" interval="10" price="0.167"/>
 <collector property="Processor.Reservation"/>
</cloudProduct>
```

Duplicate FCPorts causes IBM Systems Director to lose its zoning information for the VIOS servers

When using the collect inventory function of IBM Systems Director on an Integrated Virtual Machine (IVM) or VIOS, there could be duplicate FCPorts seen in View inventory.

Details

Duplicate FCPorts appear because the PermanentAddress attribute is being supplied in multiple cases (uppercase, mixed case, and lowercase). This prevents the creation of the proper database relationships which are needed to determine if the server has access to a storage subsystem with storage pools. Without this, you cannot perform VMControl functions, such as a workload deployment, on this IVM.

Solution

Director delivered a fix to prevent this from occurring in a new system set up, and for existing environments where this problem is occurring, they have documented a workaround. See the IBM Systems Director Technote at http://www.ibm.com/support/docview.wss?rs=0&uid=nas73e4b0a34834fa4508625790d0043f892 for the workaround details.

IBM SmartCloud Entry shows instance in 'Stopped' state even though the deployment was successful

A deployment completed successfully and the virtual server is up and running in HMC for a long period of time. However, IBM SmartCloud Entry still shows the instance state as 'Stopped'. When viewed using the IBM Systems Director VMControl user interface, the workload also shows up in a 'Stopped' state.

Details

The 'Stopped' state shown in VMControl and IBM SmartCloud Entry user interfaces is due to the fact that the IBM Systems Director server has lost access to the HMC endpoint. Until access is regained, the IBM Systems Director server will not receive any events for status changes of the physical and virtual servers managed by the HMC, which results in invalid status of these server endpoints in Director.

Solution

The administrator must revoke access to the HMC endpoint and re-request access to it. See the IBM Systems Director Technote at http://www.ibm.com/support/docview.wss?rs=0 &uid=nas7c76870211ef986e18625790e00073df7 for the workaround details.

Delete and add instance failures under load

When running under high load an occasional delete or add of an instance may fail and need to be retried by the user.

Details

If there are a large number of existing instances, and there are concurrent or near concurrent requests for deploys and/or deletes, those requests can fail with an error. You must reattempt your operation.

Solution

Retry the failed request. Ensure the management server (the server that VMware vCenter or IBM Systems Director VMControl is running on) has adequate system resources for things such as memory and CPU. (System utilities such as topas, nmon and perfmon can be used to monitor resource utilization.)

Note: (VMC only) To enable a retry of a deploy or delete failure, see “Configuring retry for a failed deploy or delete action (VMControl only)” on page 89.

Instance in Error state cannot be deleted

Instance in Error state cannot be deleted except by deleting the virtual server in IBM Systems Director.

Details

In rare circumstances an instance might fail to delete and the instance might go to the Error state in IBM SmartCloud Entry and the In Error state in IBM Systems Director VMControl. In this case the instance cannot be deleted in IBM SmartCloud Entry; the related workload must be deleted in IBM Systems Director VMControl.

Solution

Follow these steps to delete the instance and virtual server:

1. Log into IBM Systems Director.
2. Expand System Configuration and select VMControl.
3. Click Workloads and sort the workloads by State.
4. Right click on the workload with the state, In Error, and select **Related Resources** > **Server** > **Workload Employs**.

   The Navigate Resources with the virtual server associated with that workload window appears.
5. Right click on the virtual server and select **Permanently Delete Virtual Server**.

   A new tab opens with an option to **Also permanently delete all attached virtual disks**.
6. Select to **Also permanently delete all attached virtual disks** and click **OK**.

These steps delete the virtual server and workload in IBM Systems Director. When IBM SmartCloud Entry updates with IBM Systems Director, the instance in IBM SmartCloud Entry is marked “lost in cloud”. Then the instance can be deleted in IBM SmartCloud Entry.

Delete of an instance while a storage flashcopy is running against the instance will cause the delete to fail

An IBM SmartCloud Entry instance cannot be deleted immediately after the same instance has been deployed or captured.

Details

A recently deployed or captured IBM SmartCloud Entry instance has a status of "OK" and the cloud manager instance status also shows "OK", but the storage flashcopy may still be in progress, and an attempt to delete the instance while the flashcopy is running will cause the delete to fail.

Solution

To prevent an error from happening on a delete soon after a deploy or capture, you must either monitor the flashcopy until it ends, or wait for some conservative period of time, for example, 20 minutes, before attempting the delete.

The best way to tell if the flashcopy has finished is by accessing the storage subsystem user interface (UI). Here is how to use the Storwize® storage subsystem UI to determine when the flashcopy is finished:

1. Access Storwize UI.
2. From IBM SmartCloud Entry, perform the deploy or capture.
3. From the Storwize UI left navigation pane, select: Copy Services, then Flashcopy Mappings.

   A flash copy should be in progress. If a flash copy is not in progress, wait for it to be displayed; in our testing the flashcopy usually appeared about 30-60 seconds after the IBM SmartCloud Entry deploy or capture was started.
4. Wait until the flash copy completes. Once the flash copy has completed, the IBM SmartCloud Entry instance can be deleted.

IBM Systems Director unexpectedly stops logging

An incorrect value in the logging configuration can disable all logging in IBM Systems Director.

Details

When using the **lwilog** command to add a logger to the logging configuration, you must ensure that the level specified is in capitals (in other words, FINE, FINEST, ALL) and the value is a correct Java logging Level. Not specifying a correct value can result in all logging being disabled in IBM Systems Director.

Solution

See the IBM Systems Director Technote at http://www-01.ibm.com/support/docview.wss?rs=0&q1=eServerOnDemandKBRCH&q2=614294316&uid=nas7dcec2052b8c00bde8625793d0060e916&loc=en_US&cs=utf-8&lang= for the workaround details.

Failures noticed during server relocation or editing of virtual server properties

AIX virtual servers deployed from virtual appliances using IBM Systems Director VMControl 2.3.1 Storage Copy Services do not have unique UUIDs and RSCT node IDs.

Details

AIX virtual servers deployed from virtual appliances using VMControl 2.3.1 SCS do not have unique UUIDs and RSCT node IDs. When these IDs are not unique, the dynamic logical partitioning (DLPAR) function ceases to function properly, which causes VMControl functions that depend on DLPAR such as server relocation and edit virtual server to fail.

Solution

See the following IBM Systems Director VMControl Technote at http://www-01.ibm.com/support/docview.wss?rs=0&uid=nas79bec4cb3a713007c8625794b004350e5 for the workaround details.

PKI error when adding OpenStack cloud

You encounter an error message when attempting to add an OpenStack cloud to IBM SmartCloud Entry.

Details

You receive the following message when you are attempting to add an OpenStack cloud to IBM SmartCloud Entry. `Error: Unreachable Cloud :CYX6154E: An error occurred while making the OpenStack identity service token request for user 'sceagent'. The identity service responded with the following status: 500 - Error occurred when dealing with PKI token. The internal reason is '__init__() got an unexpected keyword argument 'output'' Verify that the identity service is running, and that the user name, password and tenant name are correct. Contact your system administrator for assistance.`

Solution

Due to time change on the appliance, or not using a Network Time Protocol (NTP) server, the self-signed certificates used for PKI tokens can become invalid. In order to fix the issue, ensure that the appliance operating system has the correct date and time, and then regenerate the tokens using the sceappmgr utility:

1. From the command line, run the following command: `sceappmgr`.
2. Select the **Generate Authentication Tokens** option.
3. Select **Generate New PKI Keys**.

Error opening sockets to server when using DB2

When you are running IBM SmartCloud Entry with DB2 as the database, you intermittently encounter an unexpected condition that the server cannot fulfill the request.

Details

The following specific error is displayed:

```
The server encountered an unexpected condition which prevented it from fulfilling the request
```

If you check the IBM SmartCloud Entry log you might see an exception similar to the following:

```
[05/16/13 04:38:17:009] 33904 SEVERE: CYX1846E: Internal database error.
<openjpa-2.1.0-r422266:1071316 fatal general error> org.apache.openjpa.persistence.
PersistenceException: [jcc][t4][2043][11550][4.8.87] Exception java.net.NoRouteToHostException:
Error opening socket to server localhost/127.0.0.1 on port 50,000 with message: Cannot assign
requested address. ERRORCODE=-4499, SQLSTATE=08001. Stack Trace: <openjpa-2.1.0-r422266:1071316
fatal general error> org.apache.openjpa.persistence.PersistenceException:
[jcc][t4][2043][11550][4.8.87] Exception java.net.NoRouteToHostException: Error opening socket to
server localhost/127.0.0.1 on port 50,000 with message: Cannot assign requested address.
ERRORCODE=-4499, SQLSTATE=08001
```

DB2 socket connections in TIMED_WAIT state are exhausting the available ports for DB2 connections. Normally, the system releases sockets in TIMED_WAIT state after 2 minutes. However, in some cases, this wait is too long and there are no more available sockets to use. You can reduce the amount of wait time by adjusting the TIMED_WAIT reuse and recycle values on the IBM SmartCloud Entry server.

Solution

To adjust the TIMED_WAIT reuse and recycle values on the IBM SmartCloud Entry server or appliance system, add the following to the `/etc/sysctl.conf` file:

```
net.ipv4.tcp_tw_reuse = 1
net.ipv4.tcp_tw_recycle = 1
```

Make the TIMED_WAIT reuse and recycle values effective by using the following command:

```
/sbin/sysctl -p
```

Limitations

Starting IBM SmartCloud Entry on a high scale cloud

When starting or restarting IBM SmartCloud Entry on a high scale cloud, the synchronization between IBM SmartCloud Entry and the cloud may take longer than expected. This resynchronization may cause operations such as deploying, deleting, or resizing an instance to be delayed or even fail. Wait for the synchronization to complete before attempting these actions.

Limitations when using VMware within the IBM SmartCloud Entry

- The vCenter linked mode is not supported due to limited testing. You are responsible for any errors while you are using linked vCenters mode.
- The size of a virtual disk can be increased either at deployment time or through the IBM SmartCloud Entry resize function. This increases the size of the disk, however, the guest file system is not changed and does not automatically use the increased size. To increase the guest file system to use the larger disk size, see the VMware documentation and guest operating system documentation.
- If your virtual system disks contain a Logical Volume Manager, then you must install VMware Tools inside the guest so that vCenter can customize the image during the deploy operation. For more information about LVM support, see the VMware documentation.
- All snapshots must be integrated before you create a template.
- Preferably, use shared storage for the hosts that are part of a cluster deployment target. If this is not possible, then remove hosts from the cluster while they are in maintenance mode. This prevents the default storage selection algorithm from selecting a data store that is only available from the host in maintenance mode. Selecting such a data store would cause a deployment to fail. For more information about the default storage selection algorithm, see “VMware datastore assignment during deployment” on page 92.

VMware capture instance

The capture instance function is implemented using the VMware clone to template feature. The IBM SmartCloud Entry allows you to configure the optional properties in `vmware.properties` for controlling where the new template is created when a capture request is initiated:

com.ibm.cfs.cloud.vmware.capture.image.datastore.names
Datastore(s) used when capturing the image of an instance, for example when creating a template. This list is a series of datastore names separated by commas.

com.ibm.cfs.cloud.vmware.capture.image.destination.name
The destination host or cluster for where the new template will be placed.

com.ibm.cfs.cloud.vmware.capture.image.destination.type
The type of the destination for the new template, either HOST or CLUSTER.

com.ibm.cfs.cloud.vmware.capture.image.folder

The folder path for where to place the new template, for example, . /DatacenterName/vm/FolderName.

If these properties are not specified, the default behavior is to create the new template in the same location as the existing virtual machine.

VMware storage

- When attaching a new storage volume in a cloud using VMware vCenter Server cloud, the space in assigned storage name will be ignored in the attached storage volume.
- VMControl can attach new storage only when the previous storage attachment job is complete. If you attempt to attach storage while another storage attachment job is still active, the new storage attachment fails.

DNS and domain name restrictions for VMControl AIX deployments

With VMControl AIX deployments, the network configuration requires that a DNS is always provided when a domain name is included. Likewise, if no DNS is provided, then a domain name must not be used. If this restriction is not followed, the virtual servers may end up with incorrect network settings.

Include only ASCII characters in configuration files

When editing IBM SmartCloud Entry configuration files, only use ASCII characters. If non-ASCII characters are used, the original characters are not preserved and display as garbled text in the IBM SmartCloud Entry user interface. The configuration files include all the *.properties* files in the home directory.

Maximum REST API connection limit in VMControl

VMControl 2.3.x has a maximum REST API connection limit. When you reach the limit, all requests fail with an HTTP response code of 503.

For information about how to increase the connection limit, see Performance tuning at http://publib.boulder.ibm.com/infocenter/director/sdk/index.jsp?topic=/com.ibm.usmi.dir62x.doc/dir6_2_ts_performance_tuning.html in the IBM Systems Director Information Center.

Disk resize support

In a Shared Storage Pool environment, changing the disk size when deploying is not supported. In addition, when deploying an IBM i workload, disk resize is not available. In these cases, the disk size property is not displayed in the output of `POST /cloud/api/workload` and the disk resize field is not displayed on the Advanced deployment window.

Target restrictions for VMControl IBM i deployment

Resilient system pool

When an image is deployed to create a virtual server that is running IBM i, thevirtual server must be running on a POWER7 host that has firmware release 730.51 or later and the HMC must be at version 7.7.6.0 or later.

Relocation of the resulting instance is only supported for virtual servers that are running IBM i v7.1, TR4 PTF group SF99707 level 4, or later.

Non-resilient system pool

For deployment in a system pool that is not resilient, an IBM i image does not have any special limitations. However, the deployed workload is not relocatable in VMControl.

For more information, see Deploy support and requirements in the IBM Systems Director Information Center at http://pic.dhe.ibm.com/infocenter/director/pubs/topic/com.ibm.director.vim.helps.doc/fsd0_vim_r_sb_aix_on_power_deploy_reqs_new_vs.html.

Use of network configurations provided by Network Control is not supported

Network Control has the ability to automatically deploy and move network configurations associated with virtual servers, eliminating the need for manual network configuration steps. The use of Network Control function by IBM SmartCloud Entry through VMControl is not supported in the current release.

The install path cannot contain non-English characters

When installing IBM SmartCloud Entry, the path to the installer cannot contain non-English characters.

Limitation on specifying a large memory or number of processors

When deploying an instance into a system pool, the size of memory and number of processors cannot be out of the range of the minimum or maximum value set by IBM Systems Director VMControl for that virtual server image. In addition, you cannot modify the minimum or maximum value when deploying.

To ensure the success of deployment when specifying a large memory or number of processors, follow one of these two methods:

- Modify the image manually and import it at set up time.
- Use the IBM Systems Director VMControl REST API to update the OVF maximum of an existing image. For example:

  ```
  PUT https://myserver:port/{webContext}/VMControl/virtualAppliances/{virtualApplianceOID}
  ```

  For more information about using the IBM Systems Director VMControl REST API, see IBM Systems Director VMControl SDK at http://pic.dhe.ibm.com/infocenter/director/devsdk/topic/com.ibm.vmcontrol.ws.24.doc/html/toc.html.

Limitations when you deploy an image

There are limitations when you deploy an image that is captured from a server that is configured with multiple network interfaces on the same VLAN.

Issue

A virtual machine can have one or more virtual networks. In the case where multiple network interfaces are configured on the same VLAN, VMControl captures those images under the same virtual network. For these images, VMControl deploys the network adapters that are grouped in one virtual network into one network. IBM SmartCloud Entry does not allow the user specify a different network for each network adapter. As a result, some of the network adapters do not have the network list table in IBM SmartCloud Entry. In this situation, you cannot change the VLAN mapping.

Workaround

Ensure that the virtual machine to be captured does not have multiple NICs configured on the same VLAN.

Direct usage of OpenStack CLI or REST APIs prohibited

When you use IBM SmartCloud Entry to connect to an OpenStack cloud, the direct use of any OpenStack CLI commands or REST APIs is not supported. You must use IBM SmartCloud Entry to manage OpenStack and all of the services that comprise OpenStack. Performing any management of OpenStack by using its CLI commands or REST APIs outside of IBM SmartCloud Entry might cause IBM SmartCloud Entry to malfunction and contain inconsistent data.

Unable to restore a virtual server with fixed VHD type

When a virtual server is deployed by using an image with a fixed VHD type on Hyper-V, that virtual server cannot be successfully restored after a backup.

The limitation is due to the following error condition:

```
CYX6161E: An error occurred at '2013-05-06T21:05:04Z' for virtual machine with identifier
'fd319c6e-91e9-4350-b896-9fdcd3236282'. The error code is '500'. The detailed error is:
ImageTooLarge - Image is larger than instance type allows
File "C:\Program Files (x86)\IBM\SmartCloud Entry\Hyper-V Agent\Python27\lib\site-packages\
nova\compute\manager.py", line 230, in decorated_function
return function(self, context, *args, **kwargs)
File "C:\Program Files (x86)\IBM\SmartCloud Entry\Hyper-V Agent\Python27\lib\site-packages\
nova\compute\manager.py", line 1230, in run_instance
do_run_instance()
File "C:\Program Files (x86)\IBM\SmartCloud Entry\Hyper-V Agent\Python27\lib\site-packages\
nova\openstack\common\lockutils.py", line 242, in inner
retval = f(*args, **kwargs)
File "C:\Program Files (x86)\IBM\SmartCloud Entry\Hyper-V Agent\Python27\lib\site-packages\
nova\compute\manager.py", line 1229, in do_run_instance
admin_password, is_first_time, node, instance)
File "C:\Program Files (x86)\IBM\SmartCloud Entry\Hyper-V Agent\Python27\lib\site-packages\
nova\compute\manager.py", line 877, in _run_instanceself._set_instance_error_state(context,
instance['uuid'])
File "C:\Program Files (x86)\IBM\SmartCloud Entry\Hyper-V Agent\Python27\lib\contextlib.py",
line 24, in __exit__
self.gen.next()
File "C:\Program Files (x86)\IBM\SmartCloud Entry\Hyper-V Agent\Python27\lib\site-packages\
nova\compute\manager.py",
line 798, in _run_instance
image_meta = self._check_image_size(context, instance)
File "C:\Program Files (x86)\IBM\SmartCloud Entry\Hyper-V Agent\Python27\lib\site-packages\
nova\compute\manager.py", line 1040, in _check_image_size
raise exception.ImageTooLarge()
Instance could no longer be found in the Cloud.
It could have been purposely deleted from the Cloud.
```

This issue is tracked at https://bugs.launchpad.net/nova/+bug/1177927.

Validation errors when updating a configuration strategy

When you update the configuration strategy for an image, all fields on the page are validated after you select a local file for the template, user metadata, or mapping. If any of the fields are not valid, an error message displays. Error messages display even if you have not yet provided a value for a required field, such as the mapping field. Proceed by specifying the required fields.

Accessibility

IBM SmartCloud Entry does not interfere with the accessibility features for supported browsers. For a comprehensive list of accessibility features please visit the accessibility support page for the supported browser that you are using. For a list of supported browsers, see the IBM SmartCloud Entry Administrator Guide.

The publications for this product are in Adobe Portable Document Format (PDF) and should be compliant with accessibility standards. If you experience difficulties using the PDF files and want to request a web-based format for a publication, email a request to the following address:

icfeedbk@us.ibm.com

Or, you can mail a request to the following address:

International Business Machines Corporation
Information Development
3605 Hwy 52 North
Rochester, MN, U.S.A 55901

In the request, be sure to include the publication title.

When you send information to IBM, you grant IBM a nonexclusive right to use or distribute the information in any way it believes appropriate without incurring any obligation to you.

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 grant 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.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Dept. LRAS/Bldg. 903
11501 Burnet Road
Austin, TX 78758-3400
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

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.

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. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® and ™), these symbols indicate U.S. 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 Copyright and trademark information at www.ibm.com/legal/copytrade.shtml

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or 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.

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

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

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

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

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

Privacy policy considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session and persistent cookies that collect each user's user name and password for purposes of session management, authentication, and enhanced user usability. These cookies cannot be disabled.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM's Privacy Policy at http://www.ibm.com/privacy and IBM's Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at http://www.ibm.com/software/info/product-privacy.

Printed in USA