Microsoft System Center 2012 R2

Operations Guide for App Controller in System Center 2012 Service Pack 1

Microsoft Corporation

Published: November 1, 2013

Applies To

System Center 2012

System Center 2012 Service Pack 1 (SP1)

System Center 2012 R2

Feedback

Send suggestions and comments about this document to sc2012docs@microsoft.com.

Copyright Information

Revision History

Release Date	Changes
October 17, 2013	Original release of this guide.
November 1, 2013	Minor updates to this guide.

Contents

Operations Guide for App Controller in System Center 2012 Service Pack 1 (SP1)

System Center 2012 - App Controller is a web-based management solution that lets you manage multiple public and private clouds in your organization and deploy services to them through a unified console. After deploying App Controller, you will be able to:

- Connect to and manage Windows Azure subscriptions and private clouds on System Center 2012 – Virtual Machine Manager (VMM) servers.
- Deploy and manage services and virtual machines across multiple public and private clouds.
- Manage and share file resources, service templates and virtual machine templates.
- Delegate role-based access to users for the management of services and resources on public and private clouds.

Deploying Services and Virtual Machines in System Center 2012 - App Controller

In App Controller, you can use the **Services** page to deploy new services to public and private clouds, or to change the properties of services already deployed.

The **Services** page displays the following information:

- A list of all deployed services.
- A diagram, which allows you to view or change the properties of a deployed service.
- Tasks you can perform on services deployed to public or private clouds.

In This Section

How to Deploy a Virtual Machine

Describes how to deploy a virtual machine in App Controller.

How to Deploy a Service to a Public Cloud

Describes how to deploy a service to a public cloud by using Windows Azure service packages and configuration files.

How to Deploy a Service to a Private Cloud

Describes how to deploy a service to a private cloud by using a VMM service template.

How to View a Deployed Service

Describes how to view a deployed service in App Controller.

How to Delete a Deployed Service

Describes how to remove a deployed service from public or private cloud.

How to View the Status of a Job

Describes how to view the status of tasks you perform in App Controller.

How to Copy an Existing Virtual Machine to Windows Azure

Describes how to move a virtual machine from VMM to Windows Azure in App Controller.

How to Deploy a Virtual Machine Template to Windows Azure in System Center 2012 SP1

Describes how to move a virtual machine template from VMM to Windows Azure in App Controller.

Reference

Related Sections

Setting up App Controller

Setting up Public and Private Clouds

Managing Services and Virtual Machines in System Center 2012 - App Controller

Using the Windows PowerShell module for App Controller

Overview of the App Controller Console

System Center 2012 - App Controller introduces a unified management console for managing private and public clouds and for deploying services and virtual machines.

- **Navigation pane**

  This pane is on the left side of the console and is usually the first pane you use for navigation in the console. This pane can be expanded and collapsed if you want to increase the width of a list view without changing the size of your browser window. The navigation pane contains links to the following pages:

- **Overview**—Provides access to the **Overview** page, where you can perform common management tasks and view the usage and status of private and public clouds, deployed services and virtual machines. For more information, see **Overview**.
- **Clouds**—Provides access to a list of all private and public clouds, where you can manage connections to private or public clouds and deploy services or virtual machines. For more information, see **Clouds**. Clouds can be displayed as a list or as cards.
- **Services**—Provides access to a list of all services, where you can manage deployed service configuration settings, deploy new services or virtual machines to private or public clouds, or upgrade deployed services and virtual machines. For more information, see Deploying Services and Virtual Machines in System Center 2012 - App Controller. Services can be displayed as a list or as cards.
- **Virtual Machines**—Provides access to a list of all virtual machines, where you can manage existing virtual machines or deploy new virtual machines to private clouds. This page does not contain any Windows Azure virtual machines. For more information, see Managing Services and Virtual Machines in System Center 2012 - App Controller.
- **Library**—Provides access to the App Controller library, where you can manage file shares, service templates and other resources that are required to deploy services and virtual machines to private and public clouds. For more information, see **Library**.
- **Jobs**—Provides access to a list of recent jobs, where you can view the status of tasks you have performed in App Controller. For more information, see **Jobs**.
- **Settings**—Provides access to the **Settings** node, where you can manage configuration settings for private and public cloud connections, Windows Azure subscriptions, and App Controller users and user roles. Users and user roles defined in the Settings area are applicable only to Windows Azure subscriptions. For more information, see **Settings**.

- **Header pane**

  This pane is in the top section of the console. It displays a product logo, name of the currently logged in user, link to sign out and link to Help.

- **List view pane**

  This pane is in the upper central section of the console. It displays a list of objects as appropriate for the selected item in the navigation pane.

- **Details pane**

  This pane is located in the lower central section of the console and is displayed in conjunction with list view. This pane displays summary information of an object that has been selected in the list view pane, such as a deployed service.

- **Diagram view**

  On the **Services** page and **Virtual Machines** page, use the **Open Diagram** task to view a diagram of a deployed service or virtual machine. A smaller version of the diagram is also displayed in the **Details** pane of a selected item.

- **Taskbar**

  The taskbar is located directly below the header. The taskbar displays tasks and actions appropriate to items that have been selected in other pages.

- **Status bar**

  The status bar is located directly below the list view pane or preview pane, and is displayed only when you perform a long-running task in App Controller, to let you know the status of the task. For more information about jobs in App Controller, see **Jobs**.
- **Footer**

  The footer is located at the bottom of the browser window and includes a copyright statement and a link to provide feedback to Microsoft on your experience with App Controller.

How to Deploy a Virtual Machine

Deploy a Virtual Machine

This section explains how you can deploy virtual machines on System Center 2012 – Virtual Machine Manager (VMM), on Windows Azure, or at a hosting provider. Virtual machines that are a part of a VMM service are deployed during service deployment. For VMM, this section describes how virtual machines that are not a part of a VMM service are deployed.

To deploy a virtual machine on VMM

1. On either the **Virtual Machines** page or the **Services** page, click **Deploy** in the taskbar.
2. In the **New Deployment** diagram, click **Configure** to select a cloud.
3. In the **Select a cloud for this deployment** dialog box, select a cloud and then click **OK** to return to the diagram.
4. Select a virtual machine template by clicking **Select a template**.
5. Select the appropriate virtual machine template and click **Configure**.
6. Edit the properties of the virtual machine. All fields that are required are marked by an asterisk and must be completed. For System Center 2012 SP1 only: If you want the virtual machine to access a virtual network, ensure that the virtual network is already defined before deploying the virtual machine.
7. Click **OK**, and then click **Deploy**.

   Tip

   On the **Clouds** page, if you select a VMM management server from the list and click **Deploy** in the task bar, you can start from step 4 above.

To deploy a virtual machine on a hosting provider (for System Center 2012 SP1 only)

1. On either the **Virtual Machines** page or the **Services** page, click **Deploy** in the taskbar.
2. In the **New Deployment** diagram, click **Configure** to select a cloud.
3. In the **Select a cloud for this deployment** dialog box, select a cloud and then click **OK** to return to the diagram.
4. Select a virtual machine template by clicking **Select a template**.
5. Select the appropriate virtual machine template and click **Configure**.

6. Edit the properties of the virtual machine. All fields that are required are marked by an asterisk and must be completed.
7. Click **OK**, and then click **Deploy**.

> **Tip**
> On the **Clouds** page, if you select a hosting provider from the list and click **Deploy** in the task bar, you can start from step 4 above.

To deploy a virtual machine on Windows Azure (for System Center 2012 SP1 only)

1. Do one of the following:
   - On the **Virtual Machines** page, click **Deploy** in the taskbar.
   - On the **Services** page, click **Deploy** in the taskbar.
   - On the Library page, select a virtual hard disk or an image, and then click **Deploy** in the taskbar.

     > **Caution**
     > If the virtual machine is deployed from an image in a Windows Azure container, it must be deployed to a cloud service in the same Windows Azure location.
2. In the **New Deployment** diagram, click **Configure** to select a cloud.
3. In the **Select a cloud for this deployment** dialog box, select a cloud and then click **OK** to return to the diagram.
4. In the **New Deployment** diagram, click **Configure** on the **Public Cloud** tile to select a cloud.
5. After you have selected a cloud, click **Configure** on the **Cloud Service** tile to select or create a cloud service for the virtual machine.
6. After you have selected a cloud service, click **Configure** on the **Deployment** tile.
7. In the **Properties of new deployment** dialog box, do the following
   a. Specify a name for the deployment.
   b. Select a deployment option. When you are deploying a virtual machine, the only available option is **Production**.
   c. Select a virtual network to which the virtual machine is to connect. This step is optional.
8. After you have selected a deployment option, click **Configure** on the **Virtual Machine** tile to select or create a virtual machine to deploy.
9. For System Center 2012 SP1 only: Configure the following virtual machine settings:
   - If the virtual machine is to be part of an availability set, select or create an availability set to indicate that you want virtual machines to be kept separately for improved continuity of service.
   - Set the host caching option (read/write is recommended).
   - Specify the local administrator credentials and the credentials that allow the specified

disk image to join a domain when it is deployed.

10. If you are creating a virtual machine from an image, you must also specify the destination container for the image and the Administrator password for the virtual machine.
11. After you have selected or created a virtual machine, click **Deploy** on the diagram page.

See Also

How to Upload a Virtual Hard Disk or Image to Windows Azure

How to Connect to a Virtual Machine or Service Instance by Using Remote Access

How to Connect to a Hosting Provider

How to Deploy a Service to a Public Cloud

Deploying a Service to a Public Cloud

You can start a new Windows Azure service deployment from the App Controller console by using one of the following methods:

- On the **Clouds** page:
  - Select a Windows Azure subscription from the list and click **Deploy** in the taskbar or right-click the subscription and select Deploy from the shortcut menu that appears.

    Tip
    If you start a new Windows Azure service deployment from the **Clouds** page, the Windows Azure subscription will be automatically configured as the public cloud.
- On the **Services** page:
  - Click **Deploy** in the taskbar.

    Tip
    If you start a Windows Azure service deployment from the **Services** page, you will need to select a Windows Azure subscription to configure as the Public Cloud.
- On the **Library** page:
  a. Navigate to the **Windows Azure** node in the App Controller Library.
  b. Navigate to the storage container in which the cloud service package file (.cspkg) or configuration file (.cscfg) is to be deployed.
  c. Select the package or configuration file.
  d. Click **Deploy** on the taskbar.

When you start a new service deployment, the **New Deployment** diagram view is displayed to assist you in configuring the settings for the new service deployment.

To deploy a service to a public cloud

1. Select a cloud for the deployment.

2. A cloud service is a container for your service deployments in Windows Azure. Select an existing cloud service or create a new cloud service.

   Note
   See the procedure **To create a new cloud service** for detailed information on creating new cloud services.

3. Click **Configure** to add or change the properties for this deployment. Enter a name for the deployment, select an operating system, and select an environment in which to deploy the cloud service, and then click **OK** to save the deployment properties.
4. Supply a Windows Azure service configuration file and a package file. **Configuration** files have the file name extension of .cscfg. **Package** files have the file name extension of .cspkg. These files first need to be uploaded to the Windows Azure storage account in the cloud you are deploying to. See the section **How to Copy Files From Local Shares to Public Cloud Libraries** for more information.
5. After you select a Windows Azure configuration file, the diagram is redrawn with the configuration's role. If a role requires further information to be supplied, a red asterisk is shown next to the role. Click the **Role** to open the property page and provide the additional information, which can include the instance count, certificate selection, remote desktop configuration, and custom settings.
6. The **Deploy** button will become enabled after all required properties have been specified. Click **Deploy** to deploy the service to the public cloud.

   Tip
   It can take several minutes to deploy the service. The status bar will notify you that a job has been created. Learn more about jobs in the section How to View the Status of a Job.

See Also

How to Deploy a Virtual Machine

How to Deploy a Service to a Private Cloud

How to Deploy a Service to a Private Cloud

Deploying a Service to a Private Cloud

You can start a new VMM service deployment from the App Controller console by using one of the following methods:

- On the **Clouds** page:
  - Select a VMM cloud from the list and click **Deploy** in the taskbar.

    Tip
    If you start a new VMM service deployment from the **Clouds** page, the private cloud will be automatically configured.

- On the **Services** or **Virtual Machines** page:
  - Click **Deploy** on the taskbar or right-click an existing service and select Deploy from the shortcut menu that appears.

    Tip
    If you start a VMM service deployment from the **Services** or **Virtual Machines** page, you will need to select a VMM private cloud.

When you start a new service deployment, the **New Deployment** diagram view is displayed to assist you in configuring the settings for the new service deployment.

To deploy a service to a private cloud

1. Select the cloud for deployment.
2. Select a VMM service template for the deployment.

   Note
   VMM service templates are created in the VMM Administrator console. Once created and delegated to a user role, they are available for selection within App Controller.
3. The diagram will load the service templates. Click the **Service** node in the diagram to open the service properties page. Specify a value for all required fields.
4. By default, the template will auto-generate virtual machine names and computer names for all VMM instances. If a virtual machine instance requires a specific virtual machine name or computer name, you can click **Configure** to open the property page. Within the virtual machine property page you can customize the virtual machine name and computer name.

   Note
   Some service templates have a global setting which references a computer name within the service deployment. In this case, you will have to provide a specialized computer name for the virtual machine instance to which the global setting refers.
5. The **Deploy** button will become enabled when all required settings have been supplied.

   Tip
   It can take several minutes to deploy the service. The status bar will notify you that a job has been created. Learn more about jobs in the section How to View the Status of a Job.

See Also

How to Deploy a Service to a Public Cloud

How to View a Deployed Service

To view a deployed service

1. On the **Services** page, select a service deployment.
2. Select **Open Diagram** in the taskbar or from the right-click menu to open the diagram page for the service.

   The diagram shows the structure of the deployed service, including tiers or roles and virtual machines or instances. Each of the shapes in the diagram can be clicked on to open a properties diagram.

   Right-click an item in the diagram to display a menu of all the actions available for that item.

See Also

Deploying Services and Virtual Machines in System Center 2012 - App Controller

How to Delete a Deployed Service

You can delete a deployed service from the service view. Deleting a deployed service will delete all of the instances or virtual machines that make up that deployed service.

To delete a deployed service

1. On the **Services** page, select the service deployment you want to remove.
2. Click **Delete** in the taskbar.

   Note
   A service that is deployed to Windows Azure does not need to be stopped before it is deleted.

See Also

How to Delete a Virtual Machine

How to View the Status of a Job

App Controller will periodically flush jobs from its database if the SQL Server Agent service is running.

To view the status of a job

1. To view the status of a job, click the **Jobs** node.
2. A list of jobs is displayed. Click **Show recent** or **Show all** to toggle the view of jobs to show only recent jobs (in the last 48 hours) or all jobs.

Note

The App Controller Administrator can view jobs from all users. A self-service user can only view jobs that the user has initiated.

- A friendly name for the job is displayed in the **Job** column.
- The **Target** column for a job displays the resource that was created or modified.
- The **Status** column shows the job completion status: **In Progress**, **Failed**, or **Completed**.
- The **Owner** column displays which user initiated the job.
- The **Start Time** and **End Time** columns show when the job started and ended.

When you select a job, the details of the job are displayed in the details pane below.

- For some jobs, the **Location** field displays a link to the cloud or service in which the job was performed. Clicking this link takes you to the **Clouds** or **Services** page.
- The **Job ID** is the ID of the job in the target cloud—VMM or Windows Azure. This information is useful, when following up with the VMM Administrator regarding failed jobs.
- For **Command Parameters**, click the drop-down arrow to view input parameters provided by the user.
- For failed jobs, click the **Error** drop-down arrow to display a detailed error message.

To view the status of a job in progress

1. When a job is created, App Controller displays a job notification in the status bar.
2. Click the job notification. The **Jobs** view is displayed.
3. A job in progress is displayed with the status **In Progress** in the **Status** column.

To change the retention period for job history

1. Start Windows PowerShell module for App Controller. For detailed instructions, see **Using the App Controller Cmdlets**.
2. Provide a new value for the retention period using the **Set-SCACAdminSetting** cmdlet

Note

Increasing the retention period will cause the Jobs view to take longer to open. For better performance with longer retention periods, we recommend that you archive the job table to a separate database or table.

See Also

Setting up Public and Private Clouds

How to Copy an Existing Virtual Machine to Windows Azure

This section describes how to copy a virtual machine from a VMM installation to Windows Azure. The virtual machine must be in a **Stored** state before it can be copied.

To copy an existing virtual machine to Windows Azure

1. On the **Virtual Machines** page, right-click a VMM virtual machine and click **Copy**.
2. In the **New Deployment** diagram, click **Configure** on the **Public Cloud** tile to select a cloud.
3. After you have selected a cloud, click **Configure** on the **Cloud service** tile to select a cloud service.
4. After you have selected a cloud service, click **Configure** on the **Virtual Machine** tile to configure the virtual machine.

   The virtual machine name is automatically populated from the source virtual machine. You must also specify the destination container for the virtual machine.
5. After you have configured the virtual machine, click **Deploy** on the diagram page.

See Also

How to Upload a Virtual Hard Disk or Image to Windows Azure

How to Connect to a Virtual Machine or Service Instance by Using Remote Access

How to Deploy a Virtual Machine Template to Windows Azure in System Center 2012 SP1

The information in this topic applies only to System Center 2012 SP1.

To deploy a virtual machine template to Windows Azure

1. On the Library page, select a VMM virtual machine template, and then click **Deploy** in the taskbar.
2. In the **New Deployment** diagram, click **Configure** to select a cloud.
3. In the **Select a cloud for this deployment** dialog box, select a Windows Azure cloud, and then click **OK** to return to the diagram.
4. In the Choose image for the system disk dialog box, do one of the following:
   - If the image is not yet uploaded to Windows Azure, select Upload the image that is specified in the template and specify name of the Windows Azure destination container.
   - If the image is already uploaded to Windows Azure, select **Use an existing image** and specify the image name.
5. In the **New Deployment** diagram, click **Configure** in the **Cloud Service** tile to select a cloud service to host the deployed virtual machine.
6. In the **Select a cloud service for this deployment** dialog box, select a cloud service

that is in the same location as the image that the template is using, and then click **OK**.

7. In the **New Deployment** diagram, click **Configure** in the **Virtual Machine** tile to configure the virtual machine.
8. Edit the properties of the virtual machine. All fields that are required are marked by an asterisk and must be completed.
9. Click **OK**, and then click **Deploy**.

See Also

How to Upload a Virtual Hard Disk or Image to Windows Azure

How to Connect to a Virtual Machine or Service Instance by Using Remote Access

How to Deploy a Virtual Machine

Managing Services and Virtual Machines in System Center 2012 - App Controller

In System Center 2012 - App Controller, you can use the **Virtual Machines** page to deploy or delete virtual machines and change virtual machine properties.

The **Virtual Machines** page displays the following information:

- A list of all deployed virtual machines.
- The properties of all deployed virtual machines.
- Tasks you can perform on virtual machines.

In This Section

How to View or Change the Properties of a Deployed Virtual Machine

Describes how to view or change the properties of a virtual machine.

How to Manage Virtual Machine Checkpoints

Describes how to create, delete, restore, and view the properties of the checkpoint for a virtual machine.

How to Mount an ISO File to a Virtual Machine

Describes how to mount an ISO image to the DVD drive of a virtual machine.

How to Delete a Virtual Machine

Describes how delete a virtual machine.

How to Change the Properties of a Service in a Private Cloud

Describes how to view or change the properties of a deployed VMM service.

How to Grant Access to Private Cloud Services and Virtual Machines

Describes how to grant additional users access to deployed services in VMM.

How to Change Virtual Machine State or Service Instance State

Describes how to start, stop, or make other changes to the state of a virtual machine or service.

How to Connect to a Virtual Machine or Service Instance by Using Remote Access

Describes how to use Remote Access to connect to a virtual machine.

How to Connect to a Virtual Machine by Using Virtual Machine Viewer Console Access

Describes how to view or connect a virtual machine using a console session.

How to Upgrade a Service Deployed to a Public Cloud

Describes how to upgrade a deployed service to a new version.

How to Upgrade a Service Deployed to a Private Cloud

Describes how to upgrade a deployed service to a new version.

How to Scale Deployed Services In or Out by Adding or Removing Service Instances

Describes how to add or remove capacity to scale a service.

How to Add Windows Azure Virtual Machines to a Deployed Service in System Center 2012 SP1

Describes how to scale a service by adding virtual machines in Windows Azure.

Related Sections

Setting up App Controller

Setting up Public and Private Clouds

How to View or Change the Properties of a Deployed Virtual Machine

To view or change the properties of a deployed virtual machine

1. On the **Virtual Machines** page, select a virtual machine, and then click **Properties** in the taskbar or from the right-click menu.

   Tip
   Alternatively, select a virtual machine from the list and click **Open Diagram**, and then select the virtual machine to open the **Properties** page.
2. Change the properties as desired, and then click **OK** to save your changes.

See Also

Managing Services and Virtual Machines in System Center 2012 - App Controller

How to Manage Virtual Machine Checkpoints

To manage checkpoints for a virtual machine

1. On the **Virtual Machines** page, select a virtual machine, click **Properties** in the taskbar or from the right-click menu, and then click **Checkpoints**.

   Tip
   Alternatively, select a virtual machine from the list and click **Open Diagram**, select the virtual machine to open the **Properties** page, and then click **Checkpoints**.
2. **Create**, **Delete**, **Restore**, and view the **Properties** of checkpoints as desired.

See Also

Managing Services and Virtual Machines in System Center 2012 - App Controller

How to Mount an ISO File to a Virtual Machine

How to mount an ISO file for a virtual machine

1. On the **Virtual Machines** page, select the virtual machine to which you want to mount an ISO file.
2. Click **Mount image** in the taskbar.

3. In the file selection dialog box, select an ISO file from the respective VMM library and then click **OK**.

   Note
   App Controller supports mounting ISOs only to the first DVD drive of a virtual machine.

See Also

Managing Services and Virtual Machines in System Center 2012 - App Controller

Using App Controller Library Resources

How to Delete a Virtual Machine

A virtual machine can be deleted in App Controller after it has been turned off.

To delete a virtual machine

1. On the **Virtual Machines** page, select the virtual machine to be deleted.
2. Click **Delete** from the taskbar.
3. Click **Yes** to delete the virtual machine.

See Also

Managing Services and Virtual Machines in System Center 2012 - App Controller

Deploying Services and Virtual Machines in System Center 2012 - App Controller

How to Change the Properties of a Service in a Private Cloud

To change the properties of a service in a private cloud

1. On the **Services** page, select the private cloud service to be changed.
2. Select **Open Diagram** from the taskbar or open the diagram by clicking the small diagram shown in the details pane.
3. In the diagram, click the service to open the **Properties** page for that service.
4. Make the necessary changes and then click **OK**.

   Note
   Any properties you have changed in the properties dialog will not be set until you click the **Update** button in the diagram. Clicking **Cancel** in the diagram will discard any properties that you have changed in the properties page.

   You can also change the properties of a virtual machine in the service instance within the machine tier.
5. Once you have made the changes, click the **Update** button on the diagram to commit the

changes.

See Also

How to View or Change the Properties of a Deployed Virtual Machine

How to Connect to a Virtual Machine or Service Instance by Using Remote Access

How to Connect to a Virtual Machine by Using Virtual Machine Viewer Console Access

How to Grant Access to Private Cloud Services and Virtual Machines

If additional individuals will manage a service or virtual machine, access can be granted in the properties dialog box of the service or virtual machine.

To grant users access to a private cloud service or virtual machine

1. On the **Services** page, select the service and then click **Open Diagram**. Alternatively, on the **Virtual Machines** page, select the virtual machine and then click **Open Diagram**.
2. In the diagram, select the service or virtual machine instance to update.
3. In the **Access** section, click **Add** to add a user or user role to the access list.
4. In the **Add user roles or user accounts** dialog box, you can grant access to individuals or members of a user role.
   - To grant access to an individual, enter a user name in the format of **DOMAIN\username** and then select a user role for that individual. Click **Validate** to verify that the user account exists.
   - To grant access to all members of a user role, select the user roles without entering a user name.
5. Click **OK** to add the individual or user role. When you have finished adding or removing users or roles, click **OK** to close the properties dialog box for the service or virtual machine instance.

See Also

How to Delegate Users to Public and Private Clouds

Managing User Roles

How to Change Virtual Machine State or Service Instance State

To change the state of a deployed service

1. On the **Services** page, select the service instance for which the state needs to be changed.
2. Change the state of the deployed service by clicking the appropriate button on the task bar. The available state-changing tasks are **Start**, **Stop**, **Resume**, **Suspend**, and **Shut**

down.

The state of a service deployment can also be changed in the diagram view by right-clicking a deployment and selecting an appropriate action from the menu.

To change the state of a deployed virtual machine

1. On the **Virtual Machines** page, select the virtual machine for which the state needs to be changed.
2. Change the state of the virtual machine by clicking the appropriate button on the task bar. The available state-changing tasks are **Shutdown**, **Pause**, **Turn Off**, **Save**, **Store** and **Mount image**.

   The state of a deployed virtual machine can also be changed in the diagram view by right-clicking a virtual machine instance and selecting an appropriate action from the menu.

See Also

Managing Services and Virtual Machines in System Center 2012 - App Controller

How to Connect to a Virtual Machine or Service Instance by Using Remote Access

This section describes how to access a virtual machine or service instance by using the RDP Protocol. This functionality is available only if RDP has been enabled. For VMM virtual machines, RDP is configured in the operating system; for Windows Azure instances, it is configured in the service configuration for the role.

To connect to a virtual machine

1. On the **Virtual Machines** page, select a virtual machine to which you want remote access.
2. Click **Remote Desktop**.
3. Open the downloaded RDP file to gain access.
4. In the **Diagram** view, right-click the virtual machine and select **Remote Desktop**.
5. Open the downloaded RDP file to gain access.

To connect to a Windows Azure service instance

1. On the **Services** page, select a Windows Azure service to which you want remote access.
2. In the **Diagram** view, right-click the role and select **Remote Desktop**.
3. Open the downloaded RDP file to gain access.

See Also

Managing Services and Virtual Machines in System Center 2012 - App Controller

How to Connect to a Virtual Machine by Using Virtual Machine Viewer Console Access

How to Connect to a Virtual Machine by Using Virtual Machine Viewer Console Access

To connect to a virtual machine by using Virtual Machine Viewer console access

1. On the **Virtual Machines** page, select a virtual machine to which you want console access.
2. Click **Console** in the taskbar. A console session will open for the selected virtual machine in a new browser tab or window.
3. You can also right-click a virtual machine in the list or in the diagram view and select **Console**. A console session will open for the selected virtual machine in a new browser tab or window.

   Tip
   To send the Ctrl+Alt+Del key combination, press Ctrl+Alt+End.

See Also

How to Connect to a Virtual Machine or Service Instance by Using Remote Access

Managing Services and Virtual Machines in System Center 2012 - App Controller

How to Upgrade a Service Deployed to a Public Cloud

How to Upgrade a Deployed Service in a Public Cloud

Public cloud services can be upgraded in one of two ways: an environment swap or an in-place upgrade. An environment swap places the staging environment into the production environment. As the swap occurs, the existing production environment is moved into the staging environment. An in-place upgrade replaces the existing binaries and settings with new binaries and settings.

When performing an upgrade in-place, the upgrade will be performed one upgrade domain at a time. A deployment is made up of one or more roles, which you can view in the diagram. A role's instances are automatically divided into the upgrade domains. So if your role has six instances and your deployment has two upgrade domains, the upgrade will occur on three of the role's instances at a time. Once all the instances in the upgrade domain have been upgraded, the next set of role instances is upgraded. By default the whole process of moving from upgrade domain to upgrade domain is automated. You can optionally specify that you want to manually signal when the upgrade should proceed to the next upgrade domain.

To upgrade a deployed service by swapping environments

1. On the **Services** page, select the service deployment and then select the **Upgrade** task. If you are in the diagram view of the service, right-click the deployment node and select **Upgrade**.
2. The deployment node will expand to show the staging and production environments. To move this deployment into the other environment, select the new environment and click **Upgrade**.

   Note
   A swap will only work if there is a deployment in the staging environment. If the staging environment is empty, you will not be able to perform a swap upgrade.

To upgrade a deployed service by upgrading in-place

1. On the **Services** page, select the service deployment and then select the **Upgrade** task. If you are in the diagram view of the service, right-click the deployment node and select **Upgrade**.
2. Select the new package and/or configuration file for this upgrade.
3. If a role requires information to be supplied, a red asterisk is displayed next to the role. Click the **Role** node in the diagram to open the property page. Information on this page can include the instance count, certificate selection, remote desktop configuration, and custom settings.
4. Once all required information has been supplied, click **Upgrade**.
5. After clicking **Upgrade**, you will see a confirmation dialog. If you want to manually control when the upgrade continues to the next upgrade domain, select the option on the confirmation dialog. Otherwise the upgrade will automatically move from upgrade domain to upgrade domain until the upgrade is complete.
6. If you selected the manual upgrade option, select the **Resume Upgrade** task for the service in the **Services** list view to continue to the upgrade in next upgrade domain. The **Resume Upgrade** task is only enabled when the upgrade within an upgrade domain has completed.

See Also

Managing Services and Virtual Machines in System Center 2012 - App Controller

How to Upgrade a Service Deployed to a Private Cloud

How to Upgrade a Service Deployed to a Private Cloud

Private cloud services are upgraded by selecting a new version of the service template. If your service has a status of **Pending servicing**, this selection has already been done for you by an administrator or via template authoring outside of App Controller. Canceling an upgrade for a service with the **Pending servicing** status will clear the upgrade template selection.

How to Upgrade a Deployed Service in a Private Cloud

To upgrade a deployed service

1. On the **Services** page, select the service deployment then select **Upgrade** from the taskbar. If you are in the diagram view of the service, right-click the service node and select the **Upgrade** task.
2. The **Upgrade** task displays the service diagram. Select the version of the template you want to upgrade to. If you only want to change global settings, select the same version of the template. If you want to downgrade, select an older version of the template.
3. To change global settings for the service or specify new global settings, open the service property page by clicking the hyperlink in the service node of the diagram.
4. After you have provided information for all required fields, click **Upgrade** to perform the upgrade.

See Also

Managing Services and Virtual Machines in System Center 2012 - App Controller

How to Upgrade a Service Deployed to a Public Cloud

How to Scale Deployed Services In or Out by Adding or Removing Service Instances

To scale a public cloud service deployment in or out

1. On the **Services** page, select a Windows Azure service deployment.
2. Click **Open Diagram** in the taskbar or from the right-click menu to open the diagram view for that service.
3. Select the role you want to scale in or out to open the **Properties** page.
4. Increase or decrease the number of instances for the role you selected and then click **OK**.
5. Click **Update** to save your changes. Clicking **Cancel** will discard the changes made to the role properties.

To scale out a private cloud service deployment

1. On the **Services** page, select a VMM service deployment.
2. Click **Open Diagram** in the taskbar or from the right-click menu to open the diagram view for that service.
3. Right-click the machine tier you want to scale out and select **Scale Out**.

   Note
   Not all VMM services support scale-out. This property must be set during the creation of the template by using the VMM console. If a service does not support

scale-out, the task does not appear.

4. Click **Update**. Clicking **Cancel** will discard the changes made to the role properties.

   Note
   To scale in a VMM service deployment, you must delete a virtual machine instance from the machine tier you want to scale in.

See Also

How to Deploy a Service to a Public Cloud

How to Add Windows Azure Virtual Machines to a Deployed Service in System Center 2012 SP1

This section describes how to add a virtual machine to an existing deployed cloud service in Windows Azure.

To add a virtual machine to an existing cloud service

1. On the **Services** page, click **Deploy** in the taskbar.
2. In the **New Deployment** diagram, click **Configure** to select a cloud.
3. In the **Select a cloud for this deployment** dialog box, select a cloud and then click **OK** to return to the diagram.
4. After you have selected a cloud, click **Select a package, a configuration, a blob, an image, or a disk…** on the **Deployment Type** tile and select a virtual hard disk or an image.
5. After you have selected a virtual hard disk or image, click **Configure** on the **Cloud service** tile to select a cloud service that contains one of more virtual machines.

   The service configuration diagram is displayed with a new virtual machine available to configure.
6. After you have selected a cloud service, click **Configure** on the **Virtual Machine** tile to configure the virtual machine.
7. If you are creating a virtual machine from an image, you must also specify the destination container for the image and the Administrator password for the virtual machine.
8. After you have configured the virtual machine, click **Deploy** on the diagram page.

See Also

How to Upload a Virtual Hard Disk or Image to Windows Azure

How to Connect to a Virtual Machine or Service Instance by Using Remote Access

Glossary for System Center 2012 - App Controller

Term	Definition
App Controller Library	A single logical representation of all library objects from registered clouds from VMM and Windows Azure.
capability	The ability to perform a function, for example, the ability of a cloud to host highly available virtual machines is a capability, and the ability of a cloud to connect virtual machines to a certain logical network is a capability.
capacity	A consumable resource which is pooled and reported as an aggregate value via a cloud. CPU count, memory, and storage are examples of capacity dimensions.
cloud	A pool of resources which exposes a set of capacity and capabilities without revealing the actual physical backing of the resources.
cloud resource mapping	A mapping created by an App Controller administrator with all the cloud resources.
member	An individual Active Directory user account or an Active Directory group that is assigned to one or more user roles. A user role can consist of one or more members.
portal	A website that users who are assigned to an appropriate user role can use to create and manage their own virtual machines and services.
private cloud	The cloud created within and exposed by VMM systems running within an App Controller installation's trust boundary. There can be multiple private clouds.
public cloud	A cloud provided to the general public.
quota	A per-user limit on cloud capacity usage. A quota can consist of several dimensions such

Term	Definition
	as CPUs, memory, storage, virtual machines, and so on.
scope	The set of public and private clouds to which a user role has access.
service configuration file	The file that sets values for a service. The values that you can specify include the number of instances to deploy for each role, the values for the configuration parameters that you established in the service definition file, and the thumbprints for any SSL certificates associated with the service.
service configuration setting	A configuration option that can be changed in a running service without requiring the service to be redeployed.
service definition file	The file that determines the service model, such as the roles that comprise a service, optional local storage resources, configuration settings, and certificates for SSL endpoints.
service instance	A deployed service in Windows Azure or VMM.
service package	A package, also known as a service template, is a file that contains the role binaries and the service definition file to be published to the Windows Azure fabric.
service requirement	A design option that, if it is changed, requires the service to be redeployed.
storage account	An account that provides access to Windows Azure storage services to obtain persistent, redundant storage in the cloud. The storage services include these fundamental services: a) Blob service b) Queue service c) Table service.
user profile	A profile that defines the set of available actions, scope choices, and quota options available to a user role. Examples of profiles are App Controller Administrator, Cloud Manager, and Self-Service User.
user role	A unique combination of members, scope, and quota. A user role is based on one and only

Term	Definition
	one profile.
VMM service template	A template, also called a virtual machine template, that represents a set of virtual machines that are working together to provide a tool for the customer.

Privacy Statement for System Center 2012 - App Controller

Microsoft is committed to protecting your privacy, while delivering software that brings you the performance, power, and convenience you desire in your personal computing. This privacy statement explains many of the data collection and use practices of App Controller in System Center 2012 (“App Controller”) software. It does not apply to other online or offline Microsoft sites, products, or services.

App Controller runs on Windows Server and empowers application owners to easily configure, deploy and manage services, through a common self-service experience across private and public clouds. After installing App Controller, application owners utilize a web-based interface that presents a customized view of resources based on their role in the organization, and enables them to focus on managing services rather than servers. Application owners have visibility and control of their private and public cloud services, with precise control of features at each layer.

Collection and Use of Your Information

The information we collect from you will be used by Microsoft and its controlled subsidiaries and affiliates to enable the features you are using and provide the service(s) or carry out the transaction(s) you have requested or authorized. It may also be used to analyze and improve Microsoft products and services.

We may send certain mandatory service communications such as welcome letters, billing reminders, information on technical service issues, and security announcements. Some Microsoft services may send periodic member letters that are considered part of the service. We may occasionally request your feedback, invite you to participate in surveys, or send you promotional mailings to inform you of other products or services available from Microsoft and its affiliates.

In order to offer you a more consistent and personalized experience in your interactions with Microsoft, information collected through one Microsoft service may be combined with information obtained through other Microsoft services. We may also supplement the information we collect with information obtained from other companies. For example, we may use services from other

companies that enable us to derive a general geographic area based on your IP address in order to customize certain services to your geographic area.

Except as described in this statement, personal information you provide will not be transferred to third parties without your consent. We occasionally hire other companies to provide limited services on our behalf, such as packaging, sending and delivering purchases and other mailings, answering customer questions about products or services, processing event registration, or performing statistical analysis of our services. We will only provide those companies the personal information they need to deliver the service, and they are prohibited from using that information for any other purpose.

Microsoft may access or disclose information about you, including the content of your communications, in order to: (a) comply with the law or respond to lawful requests or legal process; (b) protect the rights or property of Microsoft or our customers, including the enforcement of our agreements or policies governing your use of the services; or (c) act on a good faith belief that such access or disclosure is necessary to protect the personal safety of Microsoft employees, customers, or the public. We may also disclose personal information as part of a corporate transaction such as a merger or sale of assets.

Information that is collected by or sent to Microsoft by App Controller may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries, or service providers maintain facilities. Microsoft abides by the safe harbor framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of data from the European Union, the European Economic Area, and Switzerland.

Collection and Use of Information about Your Computer

When you use software with Internet-enabled features, information about your computer ("standard computer information") is sent to the Web sites you visit and online services you use. Microsoft uses standard computer information to provide you Internet-enabled services, to help improve our products and services, and for statistical analysis. Standard computer information typically includes information such as your IP address, operating system version, browser version, and regional and language settings. In some cases, standard computer information may also include hardware ID, which indicates the device manufacturer, device name, and version. If a particular feature or service sends information to Microsoft, standard computer information will be sent as well.

The privacy details for each App Controller feature listed in this privacy statement describe what additional information is collected and how it is used.

Security of your information

Microsoft is committed to helping protect the security of your information. We use a variety of security technologies and procedures to help protect your information from unauthorized access, use, or disclosure. For example, we store the information you provide on computer systems with limited access, which are located in controlled facilities.

Changes to this privacy statement

We will occasionally update this privacy statement to reflect changes in our products, services, and customer feedback. When we post changes, we will revise the "last updated" date at the top of this statement. If there are material changes to this statement or in how Microsoft will use your personal information, we will notify you either by posting a notice of such changes prior to implementing the change or by directly sending you a notification. We encourage you to periodically review this statement to be informed of how Microsoft is protecting your information.

For More Information

Microsoft welcomes your comments regarding this privacy statement. If you have questions about this statement or believe that we have not adhered to it, please contact us at SCACPriv@microsoft.com or:

System Center 2012 - App Controller Privacy
Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052 USA

Specific features

The remainder of this document will address the following specific features:

Windows Azure Management

What This Feature Does:

App Controller enables customers to upload Windows Azure configuration files, package files, and virtual hard drives from an on-premises deployment of Windows Server to Windows Azure. Any content you upload to Windows Azure using App Controller is governed by the use terms and privacy statement for the Windows Azure service at http://go.microsoft.com/fwlink/?linkid=236391.

Information Collected, Processed, or Transmitted:

App Controller does not separately collect any information from the user.

Use of Information:

Not applicable.

Choice/Control:

If you do not wish to upload content to Windows Azure, do not use this feature.

Windows Azure Certificate Management

What This Feature Does:

App Controller uses Windows Azure Management Certificates to authenticate requests to Windows Azure Service Management REST APIs. App Controller encrypts the certificates (.pfx certificate files) and their passwords, and stores them in the App Controller database.

Information Collected, Processed, or Transmitted:

App Controller does not separately collect any information from the user. None of this information is sent to Microsoft.

Use of Information:

Not applicable.

Choice/Control:

If you do not wish to authenticate or store certificates and passwords in this way, do not use this feature.

App Controller User Account Management

What This Feature Does:

App Controller manages users' roles for access to your Windows Azure account(s). You can add domain users to an App Controller role to access certain Windows Azure subscription accounts set up by your administrator.

Information Collected, Processed, or Transmitted:

The security ID associated with the domain account is saved in the App Controller database on a user's computer. App Controller retrieves user names and validates passwords with Active Directory. App Controller does not store user names or passwords. None of this information is sent to Microsoft.

Use of Information:

None.

Choice/Control:

If you do not wish to store this information on your computer, do not use App Controller.

App Controller User Account Caching

What This Feature Does:

App Controller encrypts the credentials of users who are currently logged on and stores the credentials in browser session cookies. This is so that you can refresh your browser session without re-entering a user name and password. Those cookies are temporary and deleted when the user logs off or closes the browser.

Information Collected, Processed, or Transmitted:

App Controller does not separately collect any information from the user. None of this information is sent to Microsoft.

Use of Information:

None.

Choice/Control:

If you do not wish to store this information in your cookies, do not use App Controller.

App Controller Administrator Auditing

What This Feature Does:

App Controller allows App Controller administrators to view objects owned by all users and tasks performed by all users.

Information Collected, Processed, or Transmitted:

None of this information is sent to Microsoft.

Use of Information:

None.

Choice/Control:

If users do not wish to share this information with your administrator(s), do not use App Controller.

Customer Experience Improvement Program

What This Feature Does:

The Customer Experience Improvement Program (“CEIP”) collects basic information about your hardware configuration and how you use our software and services in order to identify trends and usage patterns. CEIP also collects the type and number of errors you encounter, software and hardware performance, and the speed of services. We will not collect your name, address, or other contact information.

Information Collected, Processed, or Transmitted:

For more information about the information collected, processed, or transmitted by CEIP, see the CEIP privacy statement at http://go.microsoft.com/fwlink/?linkid=236393.

Use of Information:

We use this information to improve the quality, reliability, and performance of Microsoft software and services, including App Controller.

Choice/Control:

You are offered the opportunity to participate in CEIP during setup. If you choose to participate and later change your mind, you can turn off CEIP at any time by:

1. Open a Windows PowerShell window.
2. Run the following command: `Set-AdminSetting CEIPEnabled 0`.

Microsoft Error Reporting

What This Feature Does:

Microsoft Error Reporting provides a service that allows you to report problems that you may be having with App Controller to Microsoft and to receive information that may help you avoid or solve such problems.

Information Collected, Processed, or Transmitted:

For information about the information collected, processed, or transmitted by Microsoft Error Reporting, see the Microsoft Error Reporting privacy statement at http://go.microsoft.com/fwlink/?linkid=236394.

Use of Information:

We use the error reporting data to solve customer problems and improve our software and services, including App Controller.

Choice/Control:

Error reporting is configured by the operating system. You can disable error reporting at any time by use the command line `reg add "HKLM\Software\Policies\Microsoft\ Windows\Windows Error Reporting" /v Disabled /t REG_DWORD /d 1 /f` or use the registry to create or set **HKLM\Software\Policies\Microsoft\ Windows\Windows Error Reporting\Disabled (DWORD)** to a value of "1".

Important Information

Enterprise customers can use Group Policy to configure how Microsoft Error Reporting behaves on their computers. Configuration options include the ability to turn off Microsoft Error Reporting. If you are an administrator and wish to configure Group Policy for Microsoft Error Reporting, you can do so by using a Group Policy Object. Go to **Administrative Templates**, **Internet Communication Management**, and then to **Internet communication settings**, and enable **Turn off Windows Customer Experience Improvement Program**.

Microsoft Update

What This Feature Does:

Microsoft Update is a service that provides Windows updates as well as updates for other Microsoft software.

Information Collected, Processed, or Transmitted:

For details about what information is collected and how it is used, see the Update Services Privacy Statement at http://go.microsoft.com/fwlink/?LinkID=236392.

Use of Information:

For details about what information is collected and how it is used, see the Update Services Privacy Statement at http://go.microsoft.com/fwlink/?LinkID=236392.

Choice/Control:

You are offered the opportunity to turn off Microsoft Update during setup. If you have turned this feature on for another Microsoft product or service installed on Windows Server, it will be turned on by default for App Controller. You will not be presented with an opportunity to turn it off when App Controller is initially activated. However, you can turn this feature on or off at any time by following these steps:

1. Open **Control Panel**, open **System and Security**, open **Windows Update**, and then select **Change Settings**.
2. Clear the **Microsoft Update** check box.

Logo Certification for Windows Server 2008 R2

The topics in this section provide Windows Server logo certification information for System Center 2012 - App Controller.

Windows Server Logo Certification topics for App Controller

- Custom Actions in App Controller
- Windows Server 2008 R2 Logo Certification Issues for App Controller

Custom Actions in App Controller

System Center 2012 - App Controller contains the following custom actions:

- ACServer.msi

Action	Description
SchedServiceConfig	Part of Wix library. Triggers after service is configured.
SchedSecureObjects_x64	Part of Wix library. Triggers after configuring secure objects.
SchedSecureObjectsRollback_x64	Part of Wix library. Triggers rollback of secure objects.
SchedXmlFile	Part of Wix library.
ConfigureUsers	Part of Wix library. Configures users for a service.
WixSchedInternetShortcuts	Part of Wix library. Configures website shortcuts.
WixQueryOsWellKnownSID	Part of Wix library. Populates well known SID property.
CA_InfraEvents_Install	Installs ETW event publishers and logs for Infrastructure.Events.Resources.dll.
CA_InfraEvents_Uninstall	Deregisters ETW publisher for Infrastructure.Events.Resources.dll.
CA_AzureEvents_Install	Installs ETW event publishers and logs for Microsoft.SystemCenter.CloudManager.Providers.Azure.Events.Resources.dll.
CA_AzureEvents_Uninstall	Deregisters ETW publisher for Microsoft.SystemCenter.CloudManager.Providers.Azure.Events.Resources.dll.
CA_VmmEvents_Install	Installs ETW event publishers and logs for Microsoft.SystemCenter.CloudManager.Providers.Vmm.Events.Resources.dll.
CA_VmmEvents_Uninstall	Deregisters ETW publisher for Microsoft.SystemCenter.CloudManager.Providers.Vmm.Events.Resources.dll.
CA_InfraEvents_Rollback	Deregisters ETW publisher for Infrastructure.Events.Resources.dll.
CA_AzureEvents_Rollback	Deregisters ETW publisher for Microsoft.SystemCenter.CloudManager.Providers.Azure.Events.Resources.dll.
CA_VmmEvents_Rollback	Deregisters ETW publisher for Microsoft.SystemCenter.CloudManager.Providers.Vmm.Events.Resources.dll.
CA_RegisterProvider_Install	Reserves the system providers URL for the service account

Action	Description
	user.
CA_RegisterVmmProvider_Install	Reserves the VMM providers URL for the network service account.
ExecServiceConfig	Part of Wix library. Configures service.
ExecSecureObjects_64	Part of Wix library.
ExecXmlFile	Part of Wix library.
WixCreateInternetShortcuts	Part of Wix library. Configures website shortcuts.
CA_RegisterProvider_Uninstall	Deletes the system providers URL reservation for the service account user.
CA_RegisterVmmProvider_Uninstall	Deletes the VMM providers URL reservation for the network service account.
RollbackServiceConfig	Part of Wix library. Rolls back service config.
ExecSecureObjectsRollback_64	Part of Wix library. Rolls back secure objects.
ExecXmlFileRollback	Part of Wix library.
WixRollbackInternetShortcuts	Part of Wix library. Rolls back website shortcuts.
CA_RegisterProvider_Rollback	Deletes the system provider's URL reservation for the service account user.
CA_RegisterVmmProvider_Rollback	Deletes the VMM provider's URL reservation for the network service account.
CreateUserRollback	Part of Wix library. Rolls back created users.
CreateUser	Part of Wix library. Creates users.
RemoveUser	Part of Wix library. Removes users.

- ACPSModule.msi

Action	Description
WixUIValidatePath	Part of Wix library. Validate install path specified.
WixUIPrintEula	Part of Wix library. Show EULA.

Windows Server 2008 R2 Logo Certification Issues for App Controller

System Center 2012 - App Controller is certified for Windows Server 2008 R2. The following issues were identified during logo certification. None of the Windows Server 2008 R2 certification issues cause operational problems or failures in App Controller.

The following files do not contain all of the required file information (specifically, an embedded manifest):

- C:\Program Files\Microsoft System Center 2012\App Controller\Tracing\Amd64\tracefmtsm.exe

The following tools are not logo certified nor have they been tested for certification:

- TraceFmtSM.exe
- TraceLogSM.exe

The following App Controller files require administrative privileges to run:

- setup.exe
- TraceFmtSM.exe
- TraceLogSM.exe

After uninstalling App Controller, the following files will remain in the Program Files folder and are deleted when the computer is restarted:

- C:\Program Files\Microsoft System Center 2012\App Controller\Setup\Microsoft.SystemCenter.SetupTrace.dll
- C:\Program Files\Microsoft System Center 2012\App Controller\Setup\Setup.exe

The following files and folders are placed in the %TEMP%\AppController folder and they are not removed when App Controller is uninstalled. To remove them, manually delete the files.

- Authorization.Setup.dll
- Interop.WUApiLib.dll
- Microsoft.Practices.EnterpriseLibrary.Common.dll
- Microsoft.Practices.EnterpriseLibrary.Security.Cryptography.dll
- Microsoft.Practices.ServiceLocation.dll
- Microsoft.Practices.Unity.dll
- Microsoft.Practices.Unity.Interception.dll
- Microsoft.SystemCenter.CloudManager.EncryptedBasicAuthenticator.dll
- Microsoft.SystemCenter.CloudManager.Providers.System.Common.dll
- Microsoft.SystemCenter.CloudManager.SecretHelper.dll
- Microsoft.SystemCenter.CloudManager.SqmClient.dll
- Microsoft.SystemCenter.SetupFirewallException.dll
- Microsoft.SystemCenter.SetupFramework.dll
- Microsoft.SystemCenter.SetupFramework.SetupResources.dll
- Microsoft.SystemCenter.SetupTrace.dll

- Microsoft.SystemCenter.SetupWindowsUpdate.dll
- muauth.cab
- PidGenX.dll
- PKConfig-2011-05-17-01-24-18-2418.xml
- Setup.exe
- SetupConsole.exe
- SetupConsole.exe.config
- SetupLicenseManager.exe
- sqmapi.dll
- HybridCloud
- HybridCloud\ACServer.msi
- Logs
- Logs\ACPSModule.log
- Logs\ACServer.log
- Logs\AppControllerSetupWizard.log
- Logs\PrereqCheckResults.xaml
- PowerShell
- PowerShell\en
- PowerShell\en\ACPSModule.msi
- de
- de\Authorization.Setup.resources.dll
- de\Eula-Eval.rtf
- de\Eula-OEM.rtf
- de\Eula.rtf
- de\Microsoft.SystemCenter.CloudManager.EncryptedBasicAuthenticator.resources.dll
- de\Microsoft.SystemCenter.CloudManager.Providers.System.Common.resources.dll
- de\Microsoft.SystemCenter.CloudManager.SecretHelper.resources.dll
- de\Microsoft.SystemCenter.CloudManager.SqmClient.resources.dll
- de\Microsoft.SystemCenter.SetupFirewallException.resources.dll
- de\Microsoft.SystemCenter.SetupFramework.resources.dll
- de\Microsoft.SystemCenter.SetupFramework.SetupResources.resources.dll
- de\Microsoft.SystemCenter.SetupTrace.resources.dll
- de\Microsoft.SystemCenter.SetupWindowsUpdate.resources.dll
- de\Setup.resources.dll
- de\SetupConsole.resources.dll
- de\SetupLicenseManager.resources.dll
- en
- en\Eula-Eval.rtf

- en\Eula-OEM.rtf
- en\Eula.rtf
- es
- es\Authorization.Setup.resources.dll
- es\Eula-Eval.rtf
- es\Eula-OEM.rtf
- es\Eula.rtf
- es\Microsoft.SystemCenter.CloudManager.EncryptedBasicAuthenticator.resources.dll
- es\Microsoft.SystemCenter.CloudManager.Providers.System.Common.resources.dll
- es\Microsoft.SystemCenter.CloudManager.SecretHelper.resources.dll
- es\Microsoft.SystemCenter.CloudManager.SqmClient.resources.dll
- es\Microsoft.SystemCenter.SetupFirewallException.resources.dll
- es\Microsoft.SystemCenter.SetupFramework.resources.dll
- es\Microsoft.SystemCenter.SetupFramework.SetupResources.resources.dll
- es\Microsoft.SystemCenter.SetupTrace.resources.dll
- es\Microsoft.SystemCenter.SetupWindowsUpdate.resources.dll
- es\Setup.resources.dll
- es\SetupConsole.resources.dll
- es\SetupLicenseManager.resources.dll
- fr
- fr\Authorization.Setup.resources.dll
- fr\Eula-Eval.rtf
- fr\Eula-OEM.rtf
- fr\Eula.rtf
- fr\Microsoft.SystemCenter.CloudManager.EncryptedBasicAuthenticator.resources.dll
- fr\Microsoft.SystemCenter.CloudManager.Providers.System.Common.resources.dll
- fr\Microsoft.SystemCenter.CloudManager.SecretHelper.resources.dll
- fr\Microsoft.SystemCenter.CloudManager.SqmClient.resources.dll
- fr\Microsoft.SystemCenter.SetupFirewallException.resources.dll
- fr\Microsoft.SystemCenter.SetupFramework.resources.dll
- fr\Microsoft.SystemCenter.SetupFramework.SetupResources.resources.dll
- fr\Microsoft.SystemCenter.SetupTrace.resources.dll
- fr\Microsoft.SystemCenter.SetupWindowsUpdate.resources.dll
- fr\Setup.resources.dll
- fr\SetupConsole.resources.dll
- fr\SetupLicenseManager.resources.dll
- it
- it\Authorization.Setup.resources.dll

- it\Eula-Eval.rtf
- it\Eula-OEM.rtf
- it\Eula.rtf
- it\Microsoft.SystemCenter.CloudManager.EncryptedBasicAuthenticator.resources.dll
- it\Microsoft.SystemCenter.CloudManager.Providers.System.Common.resources.dll
- it\Microsoft.SystemCenter.CloudManager.SecretHelper.resources.dll
- it\Microsoft.SystemCenter.CloudManager.SqmClient.resources.dll
- it\Microsoft.SystemCenter.SetupFirewallException.resources.dll
- it\Microsoft.SystemCenter.SetupFramework.resources.dll
- it\Microsoft.SystemCenter.SetupFramework.SetupResources.resources.dll
- it\Microsoft.SystemCenter.SetupTrace.resources.dll
- it\Microsoft.SystemCenter.SetupWindowsUpdate.resources.dll
- it\Setup.resources.dll
- it\SetupConsole.resources.dll
- it\SetupLicenseManager.resources.dll
- ja
- ja\Authorization.Setup.resources.dll
- ja\Eula-Eval.rtf
- ja\Eula-OEM.rtf
- ja\Eula.rtf
- ja\Microsoft.SystemCenter.CloudManager.EncryptedBasicAuthenticator.resources.dll
- ja\Microsoft.SystemCenter.CloudManager.Providers.System.Common.resources.dll
- ja\Microsoft.SystemCenter.CloudManager.SecretHelper.resources.dll
- ja\Microsoft.SystemCenter.CloudManager.SqmClient.resources.dll
- ja\Microsoft.SystemCenter.SetupFirewallException.resources.dll
- ja\Microsoft.SystemCenter.SetupFramework.resources.dll
- ja\Microsoft.SystemCenter.SetupFramework.SetupResources.resources.dll
- ja\Microsoft.SystemCenter.SetupTrace.resources.dll
- ja\Microsoft.SystemCenter.SetupWindowsUpdate.resources.dll
- ja\Setup.resources.dll
- ja\SetupConsole.resources.dll
- ja\SetupLicenseManager.resources.dll
- pt-BR
- pt-BR\Authorization.Setup.resources.dll
- pt-BR\Eula-Eval.rtf
- pt-BR\Eula-OEM.rtf
- pt-BR\Eula.rtf
- pt-BR\Microsoft.SystemCenter.CloudManager.EncryptedBasicAuthenticator.resources.dll

- pt-BR\Microsoft.SystemCenter.CloudManager.Providers.System.Common.resources.dll
- pt-BR\Microsoft.SystemCenter.CloudManager.SecretHelper.resources.dll
- pt-BR\Microsoft.SystemCenter.CloudManager.SqmClient.resources.dll
- pt-BR\Microsoft.SystemCenter.SetupFirewallException.resources.dll
- pt-BR\Microsoft.SystemCenter.SetupFramework.resources.dll
- pt-BR\Microsoft.SystemCenter.SetupFramework.SetupResources.resources.dll
- pt-BR\Microsoft.SystemCenter.SetupTrace.resources.dll
- pt-BR\Microsoft.SystemCenter.SetupWindowsUpdate.resources.dll
- pt-BR\Setup.resources.dll
- pt-BR\SetupConsole.resources.dll
- pt-BR\SetupLicenseManager.resources.dll
- ru
- ru\Authorization.Setup.resources.dll
- ru\Eula-Eval.rtf
- ru\Eula-OEM.rtf
- ru\Eula.rtf
- ru\Microsoft.SystemCenter.CloudManager.EncryptedBasicAuthenticator.resources.dll
- ru\Microsoft.SystemCenter.CloudManager.Providers.System.Common.resources.dll
- ru\Microsoft.SystemCenter.CloudManager.SecretHelper.resources.dll
- ru\Microsoft.SystemCenter.CloudManager.SqmClient.resources.dll
- ru\Microsoft.SystemCenter.SetupFirewallException.resources.dll
- ru\Microsoft.SystemCenter.SetupFramework.resources.dll
- ru\Microsoft.SystemCenter.SetupFramework.SetupResources.resources.dll
- ru\Microsoft.SystemCenter.SetupTrace.resources.dll
- ru\Microsoft.SystemCenter.SetupWindowsUpdate.resources.dll
- ru\Setup.resources.dll
- ru\SetupConsole.resources.dll
- ru\SetupLicenseManager.resources.dll
- zh-Hans
- zh-Hans\Authorization.Setup.resources.dll
- zh-Hans\Eula-Eval.rtf
- zh-Hans\Eula-OEM.rtf
- zh-Hans\Eula.rtf
- zh-Hans\Microsoft.SystemCenter.CloudManager.EncryptedBasicAuthenticator.resources.dll
- zh-Hans\Microsoft.SystemCenter.CloudManager.Providers.System.Common.resources.dll
- zh-Hans\Microsoft.SystemCenter.CloudManager.SecretHelper.resources.dll
- zh-Hans\Microsoft.SystemCenter.CloudManager.SqmClient.resources.dll
- zh-Hans\Microsoft.SystemCenter.SetupFirewallException.resources.dll

- zh-Hans\Microsoft.SystemCenter.SetupFramework.resources.dll
- zh-Hans\Microsoft.SystemCenter.SetupFramework.SetupResources.resources.dll
- zh-Hans\Microsoft.SystemCenter.SetupTrace.resources.dll
- zh-Hans\Microsoft.SystemCenter.SetupWindowsUpdate.resources.dll
- zh-Hans\Setup.resources.dll
- zh-Hans\SetupConsole.resources.dll
- zh-Hans\SetupLicenseManager.resources.dll