Microsoft System Center 2012 R2

System Center 2012 R2 App Controller Documentation

Microsoft Corporation

Published: November 1, 2013

Authors

Curtis Love and Tabatha Marshall

Applies To

System Center 2012 - App Controller

App Controller in System Center 2012 SP1

System Center 2012 R2 App Controller

Feedback

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

Copyright

Revision History

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

Contents

Getting Started with System Center 2012 - App Controller

Setting up System Center 2012 - App Controller consists of using the System Center 2012 - App Controller Setup program to lead you through the installation process, as well as configuring user role-based security and adding resources to the App Controller Library.

Before installing App Controller, be sure that the system meets hardware and software requirements and that all prerequisite software is installed. For more information about hardware and software requirements for App Controller, see System Requirements for System Center 2012 - App Controller.

If you plan to install App Controller in a High Availability (HA) configuration, review the system requirements before beginning the installation.

An App Controller installation consists of the following features:

- One or more App Controller servers
  - Each App Controller server hosts a website console for access by using a supported browser.
- A SQL Server database
- Windows PowerShell cmdlets

In This Section

System Requirements for System Center 2012 - App Controller

Describes the hardware and software required to install and run System Center 2012 - App Controller.

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

Describes the hardware and software required to install and run App Controller in System Center 2012 SP1.

System Requirements for System Center 2012 R2 App Controller

Describes the hardware and software required to install and run System Center 2012 R2 App Controller.

What's New for App Controller in System Center 2012 Service Pack 1

Describes the new features that are available with App Controller in System Center 2012 SP1.

What's New in System Center 2012 R2 App Controller

Describes the new features that are available with System Center 2012 R2 App Controller.

App Controller Deployment Checklist

Keep track of your installation progress and make sure you don't miss any potential trouble spots in App Controller.

Related Sections

Deploying System Center 2012 R2 App Controller

Setting up Public and Private Clouds

Deploying Services and Virtual Machines

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

Using the Windows PowerShell module for App Controller

System Requirements for System Center 2012 - App Controller

Important

These system requirements are for System Center 2012 - App Controller. To see the system requirements for System Center 2012 R2 App Controller, see **System Requirements for System Center 2012 R2 App Controller**. To see the system requirements for App Controller in System Center 2012 Service Pack 1 (SP1), see System Requirements for App Controller in System Center 2012 Service Pack 1 (SP1).

System Requirements—Server

This section provides information about system requirements and supported operating systems for installing and running System Center 2012 - App Controller.

Hardware Requirements

The following are the minimum and recommended hardware requirements for the App Controller server.

Hardware component	Minimum	Recommended
Processor	Pentium 4, 2 GHz (x64)	Dual-Processor, Dual-Core, 2.8 GHz (x64) or greater
RAM	1 GB	4 GB
Hard disk space	512 MB	1 GB

Note
For better performance, we recommend that you use an instance of SQL Server installed on a different computer for the App Controller database.

Software Requirements

The following software must be installed before installing App Controller.

Software Requirement	Notes
A supported operating system	For more information, see Supported Operating Systems in this topic.
Microsoft .NET Framework 4	If .NET Framework 4 is not installed (it is not installed by default), the App Controller setup wizard will install it.
Web Server (IIS)	If the Web Server (IIS) role and the following Web Server (IIS) features are not installed, the App Controller setup wizard will install them: • Static Content • Default Document • Directory Browsing • HTTP Errors • ASP.NET • .NET Extensibility • ISAPI Extensions • ISAPI Filters • HTTP Logging • Request Monitor • Tracing • Basic Authentication • Windows Authentication • Request Filtering

Software Requirement	Notes
	• Static Content Compression • IIS Management Console
The VMM console feature in System Center 2012 – Virtual Machine Manager (VMM)	Only the VMM console feature is required for App Controller.
A supported version of SQL Server	For more information about supported versions of SQL Server, see Database Requirements in this topic.

Supported Operating Systems

Operating System	Edition	Service Pack	System Architecture
Windows Server 2008 R2 (full installation)	Standard, Enterprise, or Datacenter	Service Pack 1 or earlier	x64

Database Requirements

App Controller supports the following minimum versions of Microsoft SQL Server for hosting the App Controller database.

Supported SQL Server Edition	Service Pack	System Architecture
SQL Server 2008 R2 Datacenter		x86 and x64
SQL Server 2008 R2 Enterprise		x86 and x64
SQL Server 2008 R2 Standard		x86 and x64
SQL Server 2008 Enterprise	Service Pack 2	x86 and x64
SQL Server 2008 Standard	Service Pack 2	x86 and x64

Performance and Scale

The items below are the supported scale limits for App Controller.

Measure	Value

Maximum number of objects in a Windows Azure storage directory	900
Maximum number of VMM management servers	5
Maximum number of Windows Azure subscriptions per user	20
Maximum number of concurrent users	75
Maximum number of jobs that can be run in a 24-hour interval	10,000

Additional Information

- The computer on which you are installing the App Controller server must be a member of an Active Directory domain.
- For better performance, we recommend that you install the App Controller server on a separate computer from the VMM management server.

System Requirements—Client

This section provides information about supported operating systems for running the App Controller website.

The following software must be installed before installing the App Controller web console.

- Windows 7, Windows Vista, Windows Server 2008 or Windows Server 2008 R2
- A 32-bit browser that supports Silverlight 4
- Internet Explorer 8, Internet Explorer 9

System Requirements—Windows PowerShell Module

This section provides information about system requirements and supported operating systems for installing and running the Windows PowerShell Module for App Controller.

Software Requirements

The following software must be installed before installing the Windows PowerShell Module for App Controller.

Software Requirement	Notes
A supported operating system	For more information, see Supported Operating Systems in this topic.
Microsoft .NET Framework 3.5.1	If .NET Framework 3.5.1 is not installed (it is

Software Requirement	Notes
	not installed by default), the App Controller setup wizard will enable it for Windows Server 2008 R2 and Windows 7 only. For all other supported operating systems, you must install .NET Framework 3.5.1 manually.
Windows PowerShell 2.0	Installed by default with Windows Server 2008 R2 and Windows 7. For Windows Server 2008 and Windows Vista it must be installed manually. For more information, see KB968929 on the Microsoft Support website.

Supported Operating Systems

Operating System	Edition	Service Pack	System Architecture
Windows Server 2008 R2 (full installation)	Standard, Enterprise, and Datacenter	Service Pack 1 or earlier	x64
Windows 7	Professional, Enterprise and Ultimate	Service Pack 1 or earlier	x86 and x64
Windows Server 2008 (full installation)	Standard, Enterprise, and Datacenter	Service Pack 2	x86 and x64
Windows Vista	Professional, Enterprise and Ultimate	Service Pack 2	x86 and x64

Windows Safe Mode

App Controller does not operate and the services used by App Controller do not start if Windows is running in safe mode. If you attempt to start the App Controller services manually while in safe mode, the services fail to start and an error is written into the event log.

Preparing for Highly Available Deployments of App Controller

App Controller can be made highly available using the following methods:

- Making the database highly available by installing the database on a clustered installation of SQL Server
- Making the App Controller server highly available by either:
  - Installing multiple App Controller servers behind a load balancer

- Installing App Controller servers on a highly available virtual machine

If you are installing multiple App Controller servers behind a load balancer you will be required to configure an encryption key that is shared between the servers. After installing the first App Controller server you will need to export the encryption key by using the **Export-SCACAesKey** cmdlet and then provide it when installing subsequent servers. For more information, see Installing App Controller.

See Also

Getting Started with System Center 2012 - App Controller

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

Important

These system requirements are for App Controller in System Center 2012 Service Pack 1 (SP1). To see the system requirements for System Center 2012 R2 App Controller, see **System Requirements for System Center 2012 R2 App Controller**. To see the system requirements for System Center 2012 - App Controller, see System Requirements for System Center 2012 - App Controller.

System Requirements—Server

This section provides information about system requirements and supported operating systems for installing and running System Center 2012 - App Controller.

Hardware Requirements

The following are the minimum and recommended hardware requirements for the App Controller server.

Hardware component	Minimum	Recommended
Processor	Pentium 4, 2 GHz (x64)	Dual-Processor, Dual-Core, 2.8 GHz (x64) or greater
RAM	1 GB	4 GB
Hard disk space	512 MB	1 GB

Note

For better performance, we recommend that you use an instance of SQL Server installed on a different computer for the App Controller database.

Software Requirements

The following software must be installed before installing App Controller.

Software Requirement	Notes
A supported operating system	For more information, see Supported Operating Systems in this topic.
Microsoft .NET Framework 4	If .NET Framework 4 is not installed (it is not installed by default), the App Controller setup wizard will install it.
Web Server (IIS)	If the Web Server (IIS) role and the following Web Server (IIS) features are not installed, the App Controller setup wizard will install them: • Static Content • Default Document • Directory Browsing • HTTP Errors • ASP.NET • .NET Extensibility • ISAPI Extensions • ISAPI Filters • HTTP Logging • Request Monitor • Tracing • Basic Authentication • Windows Authentication • Request Filtering • Static Content Compression • IIS Management Console
The VMM console feature in System Center 2012 Service Pack 1 (SP1) Virtual Machine Manager	Only the VMM console feature is required for App Controller.
A supported version of SQL Server	For more information about supported versions of SQL Server, see Database Requirements in this topic.

Supported Operating Systems

Operating System	Edition	Service Pack	System Architecture
Windows Server 2008 R2 (full installation)	Standard, Enterprise, or Datacenter	Service Pack 1	x64
Windows Server 2012	Standard, Datacenter	None	X64

Database Requirements

App Controller supports the following versions of Microsoft SQL Server for hosting the App Controller database.

Supported SQL Server Edition	Service Pack	System Architecture
SQL Server 2008 R2 Datacenter	Service Pack 1 or Service Pack 2	x86 and x64
SQL Server 2008 R2 Enterprise	Service Pack 1 or Service Pack 2	x86 and x64
SQL Server 2008 R2 Standard	Service Pack 1 or Service Pack 2	x86 and x64
SQL Server 2008 Enterprise	Service Pack 2	x86 and x64
SQL Server 2008 Standard	Service Pack 2	x86 and x64
SQL Server 2012 Standard		x86 and x64
SQL Server 2012 Enterprise		x86 and x64
SQL Server 2012 Standard	Service Pack 1	x86 and x64
SQL Server 2012 Enterprise	Service Pack 1	x86 and x64

Performance and Scale

The items below are the supported scale limits for App Controller.

Measure	Value
Maximum number of objects in a Windows Azure storage directory	900
Maximum number of VMM management servers	5
Maximum number of Windows Azure subscriptions per user	20

Maximum number of concurrent users	75
Maximum number of jobs that can be run in a 24-hour interval	10,000

Additional Information

- The computer on which you are installing the App Controller server must be a member of an Active Directory domain.
- For better performance, we recommend that you install the App Controller server on a separate computer from the VMM management server.

System Requirements—Client

This section provides information about supported operating systems for running the App Controller website.

The following software must be installed before installing the App Controller web console.

- Windows Server 2012, Windows 8, Windows 7, Windows Vista, Windows Server 2008 or Windows Server 2008 R2
- A 32-bit browser that supports Silverlight 5
- Internet Explorer 8, Internet Explorer 9, Internet Explorer 10

System Requirements—Windows PowerShell Module

This section provides information about system requirements and supported operating systems for installing and running the Windows PowerShell Module for App Controller.

Software Requirements

The following software must be installed before installing the Windows PowerShell Module for App Controller.

Software Requirement	Notes
A supported operating system	For more information, see Supported Operating Systems in this topic.
Microsoft .NET Framework 3.5.1	If .NET Framework 3.5.1 is not installed (it is not installed by default), the App Controller setup wizard will enable it for Windows Server 2008 R2 and Windows 7 only. For all other supported operating systems, you must install .NET Framework 3.5.1 manually.
Windows PowerShell 3.0	Installed by default with Windows Server 2012

Software Requirement	Notes
	and Windows 8. For Windows Server 2008 R2 SP1, Windows Server 2008 SP2, and Windows 7 SP1 it must be installed manually. For more information, see KB968929 on the Microsoft Support website.

Supported Operating Systems

Operating System	Edition	Service Pack	System Architecture
Windows Server 2012	Standard, Datacenter		X64
Windows 8	basic, Pro, and Enterprise		x86 and x64
Windows Server 2008 R2 (full installation)	Standard, Enterprise, and Datacenter	Service Pack 1	x64
Windows Server 2008 (full installation)	Standard, Enterprise, and Datacenter	Service Pack 2	x86 and x64
Windows 7	Professional, Enterprise and Ultimate	Service Pack 1	x86 and x64

Windows Safe Mode

App Controller does not operate and the services used by App Controller do not start if Windows is running in safe mode. If you attempt to start the App Controller services manually while in safe mode, the services fail to start and an error is written into the event log.

Preparing for Highly Available Deployments of App Controller

App Controller can be made highly available using the following methods:

- Making the database highly available by installing the database on a clustered installation of SQL Server
- Making the App Controller server highly available by either:
  - Installing multiple App Controller servers behind a load balancer
  - Installing App Controller servers on a highly available virtual machine

If you are installing multiple App Controller servers behind a load balancer you will be required to configure an encryption key that is shared between the servers. After installing the first App Controller server you will need to export the encryption key by using the **Export-SCACAesKey**

cmdlet and then provide it when installing subsequent servers. For more information, see Installing App Controller.

See Also

Getting Started with System Center 2012 - App Controller

What's New for App Controller in System Center 2012 Service Pack 1

The following are the new features for this release of App Controller.

What's New

In App Controller in System Center 2012 Service Pack 1 (SP1), the following new features are available:

- Upload a virtual hard disk or image to Windows Azure from a VMM library or network share
- Add a virtual machine to a deployed service in Windows Azure
- Start, stop, and connect to virtual machines in Windows Azure
- Copy a virtual machine from VMM to Windows Azure
- Deploy a virtual machine in Windows Azure to create a cloud service
- Add connection to a hosting provider running Service Provider Foundation

App Controller Deployment Checklist

App Controller is simple and straightforward to install and use. However, there are always small issues that can cause problems if not addressed properly. Because explanations of these issues are scattered throughout the documentation, we've gathered them into a checklist for you. Use it to keep track of your progress and to make sure you don't forget any potential trouble spots.

App Controller Deployment Checklist

The following are the issues to which you should attend during App Controller installation and configuration.

- Before you install App Controller, you should already have configured one or more private clouds in VMM, delegated user roles to the clouds, and designated a writeable file share for each user role.
- To use Windows Azure functionality in App Controller, you should have already obtained at least one Windows Azure subscription, made a note of the subscription GUID, and created a management certificate.
- To ensure sufficient user rights during installation, the database administrator must grant at least database operator (DBO) access to a database to the user account under which App Controller is being installed.

- Make sure that you import a valid Secure Sockets Layer (SSL) certificate on the App Controller server. For evaluation purposes, you can have App Controller create a self-signed certificate during Setup.
- Any user accounts that are to administer App Controller must also be granted VMM administrator rights.
- You must create service templates in VMM before you can deploy or update VMM services using App Controller.

App Controller Maintenance Checklist

The following are the issues to which you should attend while using App Controller in production.

- After App Controller is completely installed and configured, back up the App Controller database and the database encryption key.
- To change the account under which the that App Controller services are running, you must uninstall and reinstall App Controller.
- Expired SSL production certificates can be replaced using the Internet Information Services (IIS) management console without requiring any additional configuration in App Controller.
- Whenever you create a network file share to which files will be copied from a VMM cloud library, or from which files will be copied to a VMM cloud library, then the App Controller machine account must be added to the file share permission list.

See Also

System Requirements for System Center 2012 - App Controller

Installing App Controller

Configuring App Controller

Uninstalling App Controller

Upgrading System Center 2012 - App Controller to System Center 2012 SP1

This guide will show you how to upgrade from System Center 2012 - App Controller to App Controller in System Center 2012 Service Pack 1 (SP1).

Warning

If you are planning to upgrade two or more System Center components, it is important to start by reading the guide **Upgrade Sequencing for System Center 2012 SP1**. The order in which you perform component upgrades is important. Failure to follow the correct upgrade sequence might result in component failure for which no recovery options exist. The affected System Center components are:

1. Orchestrator

2. Service Manager
3. Data Protection Manager (DPM)
4. Operations Manager
5. Configuration Manager
6. Virtual Machine Manager
7. App Controller

See Also

Tasks to Perform Before You Begin the Upgrade

How to Upgrade to App Controller in System Center 2012 Service Pack 1

Troubleshoot an App Controller Upgrade

Tasks to Perform Before You Begin the Upgrade

Before you can upgrade App Controller to the Beta version of System Center 2012 Service Pack 1 (SP1), you must prepare the environment by performing the following tasks:

1. Complete all jobs running in the current App Controller installation. For information about viewing jobs, see the How to View the Status of a Job topic in the App Controller library on TechNet.
2. Ensure that VMM is upgraded before you proceed. For more information on this and other System Center 2012 SP1 upgrades, see the guide Upgrade Sequencing for System Center 2012 SP1.
3. Ensure that there are no pending restarts on the computer on which the App Controller server is installed. For example, if you have installed a server role by using Server Manager or have applied a security update, you may need to restart the computer. After you have restarted the computer, log on to the computer with the same user account to finish the installation of the server role or the security update.
4. Perform a full backup of the App Controller database. For information about backing up the App Controller database, see the How to Back up and Restore System Center 2012 - App Controller topic in the App Controller library on TechNet. You can also use tools provided by SQL Server to back up the VMM database. For more information, see Backing Up and Restoring Databases in SQL Server.
5. Upgrade the hardware, operating system, and other software if necessary to meet the requirements of App Controller in System Center 2012 SP1.
6. Upgrade VMM.

See Also

How to Upgrade to App Controller in System Center 2012 Service Pack 1

Troubleshoot an App Controller Upgrade

How to Upgrade to App Controller in System Center 2012 Service Pack 1

This guide will show you how to upgrade from System Center 2012 - App Controller to App Controller in System Center 2012 Service Pack 1 (SP1).

Warning

If you are planning to upgrade two or more System Center components, it is imperative that you first consult the guide Upgrade Sequencing for System Center 2012 SP1 (http://go.microsoft.com/fwlink/p/LinkId=262694). The order in which you perform component upgrades is important. Failure to follow the correct upgrade sequence might result in component failure for which no recovery options exist. The affected System Center components are:

1. Orchestrator
2. Service Manager
3. Data Protection Manager (DPM)
4. Operations Manager
5. Configuration Manager
6. Virtual Machine Manager
7. App Controller

Before you begin, ensure that VMM has already been upgraded to System Center 2012 SP1.

Important

In order to install or upgrade the App Controller server, you must be logged in as a domain user with membership in the local Administrators group, or equivalent, on the computer that you are configuring. This account must also have at least DBO permission on the database that will be used.

To upgrade App Controller to System Center SP1 Beta

1. Upgrade any App Controller prerequisites that have changed. This includes upgrades to Windows Server 2012 of SQL Server 2012
2. Start the Setup program for the App Controller Beta release.
3. Click Install and follow the Setup instructions.

See Also

Tasks to Perform Before You Begin the Upgrade

Troubleshoot an App Controller Upgrade

Troubleshoot an App Controller Upgrade

For general information about troubleshooting App Controller, see the topic Troubleshooting System Center 2012 - App Controller in the App Controller library on TechNet.

Log Files

If there is a problem during upgrade, consult the log files that are located in the %LOCALAPPDATA%\AppController\Logs folder.

Known Issues

For a list of the known issues, including deployment issues, for App Controller in System Center 2012 SP1, see the Release Notes for App Controller in System Center 2012 SP1 topic in the App Controller library on TechNet.

See Also

Tasks to Perform Before You Begin the Upgrade

How to Upgrade to App Controller in System Center 2012 Service Pack 1

Deploying System Center 2012 R2 App Controller

Setting up System Center 2012 - App Controller consists of using the System Center 2012 - App Controller Setup program to lead you through the installation process, as well as configuring user role-based security and adding resources to the App Controller Library.

Before installing App Controller, be sure that the system meets hardware and software requirements and that all prerequisite software is installed. For more information about hardware and software requirements for App Controller, see System Requirements for System Center 2012 - App Controller.

If you plan to install App Controller in a High Availability (HA) configuration, review the system requirements before beginning the installation.

An App Controller installation consists of the following features:

- One or more App Controller servers
  - Each App Controller server hosts a website console for access by using a supported browser.
- A SQL Server database
- Windows PowerShell cmdlets

In This Section

Installing App Controller

Describes how to deploy App Controller.

Configuring App Controller

Describes how to configure App Controller.

How to Back up and Restore System Center 2012 - App Controller

Describes how to prepare App Controller for disaster recovery.

Uninstalling App Controller

Describes how to uninstall App Controller.

Managing User Roles

Describes how to create and manage user roles in App Controller.

Using App Controller Library Resources

Describes how to manage the App Controller Library.

Setting up Public and Private Clouds

Describes how to manage your public and private cloud connections, and connections to hosting service providers. Support for hosting service providers is available only in System Center 2012 Service Pack 1 (SP1).

How to Install a Language Pack

Describes how to install a language pack for App Controller to work in a different language.

Related Sections

Deploying Services and Virtual Machines

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

Using the Windows PowerShell module for App Controller

Installing App Controller

This section provides step-by-step instructions for installing System Center 2012 - App Controller. After you install App Controller, see the section Configuring App Controller for instructions on how to configure App Controller.

To install the App Controller server, see the section How to Install the App Controller Server. To install the Windows PowerShell Module for App Controller, see the section How to Install the Windows PowerShell Module for App Controller.

How to Install the App Controller Server

The procedures in this section describe how to install System Center 2012 - App Controller server.

Before you begin the installation of App Controller server, ensure that you have a computer with a supported version of Microsoft SQL Server installed and running. If you require support for 4 byte Unicode strings, ensure before installing that the database collation is set to one of the _100_ collations; for example, Chinese_Simplified_Pinyin_100_. If you do not want to set the entire SQL Server database to have a _100_ collation, create an empty database for App Controller to use, and then set the collation sequence of that database to be one of the _100_ collations. A full list of _100_ collations is available from the Windows Collation Name topic in the Transact-SQL Reference on MSDN.

Note

If there is a problem with Setup completing successfully, consult the log files that are located in the %LOCALAPPDATA%\AppController\Logs folder (for System Center 2012 - App Controller) or \ProgramData\AppControllerLogs (for App Controller in System Center 2012 SP1).

In order to install the App Controller server, you must be logged in as a domain user with membership in the local Administrators group, or equivalent, on the computer that you are configuring. This account must also have at least DBO permission on the database that will be used.

To install the App Controller server

1. On your installation media, right-click **setup.exe**, and then click **Run as administrator**.

   Note

   Before beginning the installation of App Controller, close any open programs and ensure that there are no pending restarts on the computer. For example, if you have installed a server role by using Server Manager or have applied a security update, you may need to restart the computer and then log on to the computer with the same user account to finish the installation of the server role or the security update.

2. On the main setup page, click **Install**.

3. On the **Product registration information** page, provide the appropriate information and then click **Next**. Review the license terms, select the **I have read, understood, and agree with the terms of the license agreement** check box, and then click **Next**.
4. The computer on which you are installing the App Controller server will be checked to ensure that the appropriate hardware and software requirements are met. If a prerequisite is not met, a page will appear with information about which prerequisite has not been met and how to resolve the issue. If all prerequisites have been met, the **Select the installation location** page will appear.

   For information about hardware and software requirements for App Controller, see System Requirements for System Center 2012 - App Controller.
5. On the **Select the installation location page**, use the default path or select a different installation path for the App Controller program files, and then click **Next**.
6. On the **Configure services** page, specify the account that will be used by App Controller services. You can configure App Controller services to use either the Network Service account or a domain account.

   Note
   If you specify a domain account, it is strongly recommended that you create an account that is specifically designated to be used by App Controller services.

   You can also configure the port that will be used by App Controller services.

   Note
   This port is used for communication between App Controller services only. You do not need to configure the firewall on the computer running App Controller to allow access to this port.
7. On the **Configure website** page, specify the following:
   - **IP address**: Select an IP address from the IP address list or type an IP address that users can use to access this site.
   - **Port**: Type the port on which HTTP.sys must listen for requests made to this website. If you specify a port different from the default port (443 for HTTPS), clients must specify the port number in requests to the server or they will not connect to the Web site.
   - **SSL certificate**: Select whether you want App Controller Setup to generate a self-signed certificate or use a previously imported certificate for SSL.

     Note
     To add or configure server certificates, use the **Server Certificates** feature in IIS Manager.

     If you use a self-signed certificate, the certificate must be added to the Trusted Root Certification Authorities store of all computers that will access the App Controller website. Some browsers will fail to display App Controller if the certificate is not trusted. It is recommended that you use a certificate from a trusted certification authority instead of using a self-signed certificate.

Important

The port that you assign during the installation of App Controller cannot be changed without uninstalling and reinstalling App Controller.

After you have configured the website binding to be used by the App Controller server, click **Next**.

8. On the **Configure the database** page, specify the following:
   - **Server name**: Type the name of the computer that is running SQL Server. If you are installing the App Controller server on the same computer that is running SQL Server, the **Server name** will be prepopulated with the name of the computer.
   - **Port**: Type the port to use for communication with the computer that is running SQL Server. By default, this value is not required and is therefore left blank.
   - **Instance name**: Select or type the name of the instance of SQL Server to use. There will be a short delay while the instance names are populated in the list. The list of available instances may not correspond to the **Port** specified above.
   - **Database name**: Type the name of the database to use. The account with which you are installing the App Controller server must have at least database owner (dbo) permissions in the specified database. If the specified database does not exist and the current user has the appropriate permissions, the App Controller setup wizard will create it for you. If you are performing a high availability installation, the second and subsequent server installs need to use the same database as the first server.

     Note

     Only one App Controller database can be installed per SQL Server instance.

   After you have configured the database to be used by the App Controller server, click **Next**.
9. On the **Configure encryption key** page, select the exported encryption key file and provide the appropriate password, and then click **Next**. These two values are specified when exporting the encryption key from an existing App Controller installation.

   Note

   This screen will only appear when using an existing App Controller database. This is required if you are setting up a highly available deployment of App Controller. Use the **Export-SCACAesKey** cmdlet to export the encryption key. See **Using the Windows PowerShell Module for App Controller** for more information on how to use cmdlets.
10. On the **Help improve System Center 2012 - App Controller** page, select whether or not you want to opt-in to the Customer Experience Improvement Program (CEIP) and use Microsoft Update, and then click **Next**.

    Note

    If you have previously chosen to use Microsoft Update on this computer or it is enabled by Group Policy, the option may be disabled.
11. On the **Confirm the settings** page, review your selections and do one of the following:

- Click **Previous** to change any selections.
- Click **Install** to install the App Controller server.

After you click **Install**, the **Installing components** page appears and installation progress is displayed.

12. On the **Setup completed successfully** page, do one of the following:
    - To open the App Controller website when you close the setup wizard, ensure that the **Start the App Controller website when Setup closes** check box is selected.
    - Click **Finish**.

If Setup is unable to complete, you are provided with a list showing which items could not be installed, along with links to the related log files. Review these logs for more information about where the Setup issue occurred. For additional information about Setup issues, see Troubleshooting System Center 2012 - App Controller and the Installation section of the Release Notes for System Center 2012 - App Controller.

How to Enable Single Sign-On for App Controller

By default, App Controller is enabled to prompt users to sign in by entering their Active Directory user name and password. The following procedures describe how to configure App Controller to use the user's current Windows credentials to automatically sign on.

To verify or change the authentication method

1. Open IIS manager on the App Controller server.
2. Select the App Controller website.
3. Expand the website and select the **/api** node.
4. Click **Authentication**.
5. Enable Windows Integrated Authentication.
6. Disable Basic Authentication.

To turn on constrained delegation

1. Log on using an account that has OU Administrator privileges in Active Directory Domain Services. Ensure that this account is also granted the **SeEnableDelegationPrivilege** user right (for example, a domain administrator could run the command `ntrights -u domain\user +r SeEnableDelegationPrivilege` on a domain controller, where domain/user represent the domain and account name for the account).
2. In Active Directory Users and Computers, expand the App Controller Machine node.
3. Click the **Delegation** tab.
4. Select the **Trust this computer for delegation to specified services only** option.
5. Select the **Use any authentication protocol** option.
6. Click Add and then do one of the following:
    a. If the VMM management server is running under the Local System account, enter the

name of the VMM management server and select **HOST**, and then click **OK**.

b. If the VMM management server is running under a domain account, enter the name of domain account and select **SCVMM**, and then click **OK**.

7. Select the Common Internet File System (CIFS) service, and then click OK.
8. Restart the App Controller management server.

How to Install the Windows PowerShell Module for App Controller

The procedures in this section describe how to install the Windows PowerShell Module for App Controller.

Before you begin the installation of the Windows PowerShell Module for App Controller, ensure that you have a computer with a supported version of Windows PowerShell installed or enabled.

Membership in the local Administrators group, or equivalent, on the computer that you are configuring is the minimum requirement to complete this procedure.

To install the Windows PowerShell module for App Controller

1. On your installation media, right-click **setup.exe**, and then click **Run as administrator**.
2. On the main setup page, click **Install Windows PowerShell module for App Controller**.
3. On the **End-User License Agreement** page, review the license terms, select the **I accept the terms in the License Agreement** check box, and then click **Next**.
4. Click **Install** to install the Windows PowerShell Module for App Controller.
5. Verify the installation results and then click **Finish**.

How to Use a Command Prompt to Install App Controller

You may prefer to install App Controller at the command prompt if you want to install App Controller without user intervention.

Use the Setup.exe program in the Installation folder of the product CD to install and uninstall App Controller at a command prompt. The following sections list the various parameters you can use with Setup.exe. Command-line parameters can be used in any order.

Tip

Uninstalling App Controller using the command line will always delete the database. If you need to retain the database, use the interactive UI.

App Controller Command-Line Installation Parameters

The following table describes the parameters you can use with Setup.exe to install App Controller.

Parameter	Required	Description
/help or **/?**	Optional	Displays the Help dialog box.
/Silent	Optional	Specifies to install the product without displaying the user interface. Runs Setup interactively if not specified.
/SelfUpdate <*Boolean*>	Optional	Checks for product updates from Microsoft Update before starting Setup. Does not check for updates if not specified.
/InstallPath<*path*>	Optional	Specifies the folder location for installing the App Controller binaries. Uses **%PROGRAMFILES%\Microsoft System Center 2012\App Controller** if not specified.
/ProductKey<*ProductKey*>	Optional	Specifies the Microsoft product key supplied with your purchase of App Controller. If not specified, App Controller will be in evaluation mode.
/ServiceUsername<*domain*>\<*username*>	Optional	Specifies the account used to run App Controller processes.
/ServicePassword<*password*>	Optional	Specifies the **ServiceUsername** account password.
/ServicePort<*port*>	Optional	Specifies the port used to run App Controller processes. Uses port 18622 if not specified.
/IP<*IP address*>	Optional	Specifies the IP address for the App Controller website binding. Uses all unassigned IP addresses if not specified.
/Port<*port*>	Optional	Specifies the port for the App Controller website binding.

Parameter	Required	Description
		Uses 443 if not specified.
/SslCert <*hash*>	Optional	Specifies the SSL certificate for the App Controller website binding. Generates a self-signed certificate if not specified.
/SQL <*server*>,<*port*>\<*instance*>	Required	Specifies the Microsoft SQL Server name and instance where the App Controller database is to be installed.
/SQLdb <*database*>	Optional	Specifies the Microsoft SQL Server database name for the App Controller database. Uses the name **AppController** if not specified.
/AesKeyFilePath <*path*>	Required only when using an existing database	Specifies the AES key used to encrypt and decrypt values in the App Controller database.
/AesKeyPassword <*password*>	Required only when using an existing database	Specifies the password used to decrypt the AES key file.
/CEIP	Optional	Enables App Controller to send anonymous feedback to Microsoft as part of the Customer Experience Improvement Program. Does not enroll in CEIP if not specified.
/MU	Optional	Configures the server to use Microsoft Update. Does not enroll in Microsoft update if not specified.
/acceptEula	Mandatory	Indicates that you have read, understood, and agree with the license terms.

Example: Install App Controller

Use the following code example to install App Controller:

```
Setup.exe /Silent /SelfUpdate true /InstallPath "C:\AppController" /ServiceUsername
"CONTOSO\AppControllerSrvAcct" /ServicePassword "P4ssw0rd!" /ServicePort 18623 /IP
10.1.2.3 /Port 444 /SslCert 2d8bfddf59a4a51a2a5b6286c22473108395624d /SQL
"CONTOSOSQLSRV,1434\Instance1" /SQLdb AppControllerDatabase /AesKeyFilePath
"C:\backup\AppControllerAesKey" /AesKeyPassword "P4ssw0rd$" /CEIP /MU /acceptEula
```

See Also

Configuring App Controller

Uninstalling App Controller

Troubleshooting System Center 2012 - App Controller

Release Notes for System Center 2012 - App Controller

Configuring App Controller

Opening the App Controller Console

To use the App Controller console, client computers must be running a supported browser.

By default, users and groups in the local Administrators group are members of the App Controller Administrator role. Before other users can access the App Controller console, an App Controller Administrator must do one of the following:

- Connect App Controller to a VMM management server.
- Connect a Windows Azure subscription and create a self-service user role.

For more information about connecting VMM management servers, connecting Windows Azure subscriptions, and creating self-service user roles, see Managing Services and Virtual Machines in System Center 2012 - App Controller.

To open the App Controller console in a Web browser

1. In a Web browser, specify the console website in one of the following formats:
   - If the console website is using a non-default port, type **https://** followed by the computer name of the web server, a colon (:), and then the port number. For example, type **https://webserver:444**.
   - If the console website is not using a dedicated port, then type **https://** followed by the host header name.
2. If Silverlight 5 is not installed, click the graphic to download and run the installer.
3. On the logon page, provide the appropriate credentials, and then click **Sign in**. If single sign on is enabled you will not be prompted for credentials.

4. If you are a member of multiple user roles you will need to select a user role that will apply for this session. You can quickly change user roles by refreshing the browser window.

Customize the Organization Logo

You can customize the organization logo of the App Controller console.

To customize the organization logo

1. Navigate to the website root of the App Controller installation directory. By default, this is **%PROGRAMFILES%\Microsoft System Center 2012\App Controller\wwwroot**.
2. Create a backup of the default organization logos by renaming the files as follows:
   a. Rename **SC2012_WebHeaderLeft_AC.png** to **SC2012_WebHeaderLeft_AC.png.old**
   b. Rename **SC2012_WebHeaderRight_AC.png** to **SC2012_WebHeaderRight_AC.png.old**
3. Copy your logo into the **wwwroot** folder.

   The images must meet the following requirements:

Location	Image Name	Size
Top left	**SC2012_WebHeaderLeft_AC.png**	287x44
Top right	**SC2012_WebHeaderRight_AC.png**	108x16

Note
The format must be PNG with a transparent background.

See Also

Getting Started with System Center 2012 - App Controller

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

How to Back up and Restore System Center 2012 - App Controller

Other than that which is contained in the App Controller database, the App Controller server retains no information that requires a backup. The database can be restored in an existing environment without running App Controller Setup. You should run App Controller Setup again only for disaster recovery; specifically, to reinstall App Controller using an existing database.

To back up the App Controller database

1. Start Windows PowerShell module for App Controller. For detailed instructions, see **Using the App Controller Cmdlets**.
2. Export the App Controller Advanced Encryption Standard (AES) key using the **Export-SCACAesKey** cmdlet.
3. Use standard database tools, such as SQL Server Management Studio, to back up the App Controller database.

To restore the App Controller database

1. Use standard database tools, such as SQL Server Management Studio, to restore the App Controller database.
2. If you run App Controller Setup again as part of a disaster recovery process, provide Setup with the AES key file that was exported during backup.

See Also

Getting Started with System Center 2012 - App Controller

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

Uninstalling App Controller

How to Uninstall the App Controller Server

You can use the following procedure to uninstall the App Controller server. Membership in the local Administrators group, or equivalent, on the computer that you are configuring is the minimum required to complete this procedure.

Note

If there is a problem with setup completing successfully, consult the log files that are located in the **%LOCALAPPDATA%\AppController\logs** folder.

To report a problem, go to the Submit Feedback page on Microsoft Connect. You must be a registered App Controller program participant on Microsoft Connect to report a problem.

To uninstall the App Controller server

1. On the computer on which the App Controller server is installed, click **Start**, and then click **Control Panel**.
2. Under **Programs**, click **Uninstall a program**.
3. Under **Name**, double-click **System Center 2012 - App Controller**.
4. On the **Repair or Uninstall App Controller** page, select whether or not you want App Controller Setup to delete its SQL Server database during uninstallation, and then click **Uninstall**.

Note

If you chose not to delete the SQL Server database, you will be required to provide a path to export the encryption key and a password to encrypt the file. To reuse this database for a subsequent installation of App Controller you will need to use this encryption key and password.

After you click **Uninstall**, the **Uninstalling components** page appears and uninstallation progress is displayed.

5. After the App Controller server is uninstalled, on the **Uninstall completed successfully** page, click **Close**.
6. If you are planning to reinstall the App Controller server, restart the computer.

Uninstalling App Controller will not remove certificates for VMM library servers. For more information about removing certificates, see How to Remove Certificates for VMM Library Servers.

How to Uninstall the Windows PowerShell Module for App Controller

You can use the following procedure to uninstall the Windows PowerShell Module for App Controller.

Membership in the local Administrators group, or equivalent, on the computer that you are configuring is the minimum required to complete this procedure.

Note

Uninstalling the App Controller server will also uninstall the Windows PowerShell module.

To uninstall the Windows PowerShell Module for App Controller

1. On the computer on which the App Controller server is installed, click **Start**, and then click **Control Panel**.
2. Under **Programs**, click **Uninstall a program**.
3. Under **Name**, double-click **Windows PowerShell Module for App Controller**, and then click **Yes**.

See Also

How to Remove Certificates for VMM Library Servers

Managing User Roles

System Center 2012 - App Controller adds user role management capabilities for Windows Azure subscriptions or hosting service providers while also respecting user roles created in System Center 2012 – Virtual Machine Manager. Only user roles for Windows Azure

subscriptions or hosting providers can be created in App Controller. VMM Administrators must manage VMM user roles by using the VMM console.

Important
Support for hosting service providers is available only in System Center 2012 Service Pack 1 (SP1).

In This Section

About User Roles in App Controller

Describes the types of user roles and which tasks they can perform in App Controller.

How to Manage the Administrators User Role

Describes how to add or remove users from the App Controller Administrators user role.

How to Create a User Role in App Controller

Describes how to create a user role in App Controller.

See Also

How to Delegate Users

About User Roles in App Controller

Understanding User Roles in App Controller

There are two types of user roles in App Controller.

User Role	Permissions
Administrator	Members of the Administrators user role can perform all administrative actions on all App Controller objects. This is a built-in group and cannot be deleted or renamed. **Note** VMM administrators in connected VMM management servers are not automatically added to the App Controller Administrators user role. During Setup, this role is automatically

User Role	Permissions
	populated with all supported users and groups in the local Administrators group of the computer on which App Controller is installed.
Self-Service User	Administrators can create one or more Self-Service user roles in which to delegate user access to Windows Azure subscriptions or hosting service providers. Self-Service users can deploy and manage services only to Windows Azure subscriptions or hosting service providers to which they have access. **Important** Support for hosting service providers is available only in System Center 2012 Service Pack 1 (SP1). Additionally, Self-Service user roles can be designated as Read-only for the specified scope.

See Also

[How to Manage the Administrators User Role]
[How to Create a User Role in App Controller]

How to Manage the Administrators User Role

The procedure in this section explains how to manage the Administrators user role in App Controller. Members of the Administrators user role in App Controller are not granted Administrator privileges in connected VMM servers unless they were specifically granted those permissions in VMM.

To add members to the Administrators user role

1. In the **Settings** node, click **User Roles**, select the **Administrators** user role, and then click **Properties**.
2. On the **Members** tab, click **Add**.
3. In the **Select Users or Groups** dialog box, enter an Active Directory user account or security group name and then click **Add**. Each user or security group must be added one at a time.

   Note
   Use the format **domain\user**.

When you have finished adding users or groups, click **OK**.

To remove members from the Administrators user role

1. In the **Settings** node, click **User Roles**, select the **Administrators** user role, and then click **Properties**.
2. On the **Members** tab, select a member to remove and then click **Remove**. When you have finished removing users or groups, click **OK**.

See Also

Managing User Roles

How to Create a User Role in App Controller

The procedures in this section explain how to create a user role that can deploy and manage services to one or more Windows Azure subscriptions or hosting providers.

To create a user role

1. In the **Settings** node, click **User Roles**, and then click **New**.
2. On the **General** tab, specify a **User role name** and **Description**. Then specify whether or not this user role is a **Read-only role**. A read-only role will not be able to make any changes to a Windows Azure subscription.
3. On the **Members** tab, add Active Directory users or groups to the role.
4. On the **Scope** tab, do one or both of the following:
   - Select any Azure subscriptions that you want the user role to access.
   - For System Center 2012 SP1 only: Under **Service provider connections**, select any hosting service providers that you want the user role to access.
5. Click **OK**.

See Also

How to Delegate Users

Using App Controller Library Resources

In System Center 2012 - App Controller, you can use the **Library** page to manage file shares, templates, and resources for both System Center 2012 – Virtual Machine Manager (VMM) and Windows Azure.

The **Library** page displays a tree view of all libraries. By default, the root **Library** node is expanded to display the container nodes for **Shares** and **Cloud Libraries**.

Tip

For more detailed information about the structure and content of the App Controller Library, see About the App Controller Library in this section.

In This Section

About the App Controller Library

The App Controller Library is a collection of resources in which users can move, store, and share objects associated with VMM or Windows Azure clouds.

How to Add or Remove File Shares in the App Controller Library

Describes how to add or remove file shares in App Controller.

How to Add or Remove a Windows Azure Storage Account

Describes how to add or remove a Windows Azure storage account in App Controller.

How to Add or Remove a Windows Azure Storage Container

Describes how to add or remove a Windows Azure storage container in App Controller.

How to Copy Files from Shares to Public Clouds

Describes how to copy a file from a share to a public cloud in App Controller.

How to Copy Files from Shares to Private Clouds

Describes how to copy a file from a share to a private cloud in App Controller.

How to Deploy a Virtual Machine Template to a Private Cloud

Describes how to deploy a virtual machine template from the App Controller Library to a private cloud.

How to Copy Library Resources Between Clouds of the Same Type

Describes how to copy templates, storage containers, and other resources in App Controller.

How to Refresh VMM Library Server Certificates

Describes how to import SSL certificates when a new library server is added to the App Controller Library.

Related Sections

Deploying Services and Virtual Machines

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

See Also

Managing Connection Settings

Managing Windows Azure Subscription Settings

How to Connect to Public Clouds

How to Deploy a Virtual Machine

About the App Controller Library

The App Controller Library is a collection of resources associated with VMM or Windows Azure clouds that users can move, store, and share.

App Controller makes available three types of shared storage:

- File shares on your network
- Private cloud libraries
- Windows Azure storage accounts

Shares

The **Shares** node can contain a list of network file shares added to App Controller by administrators. Both administrators and self-service users can store files and resources they intend to move into public or private clouds. Access control to a share is managed by the file server. Administrators can add or remove file shares in the App Controller Library. Self-service users with proper permission are allowed to create or delete folders in a share, and copy and paste files between shares. Files can be copied from local shares to public or private cloud libraries.

To copy resources from a network file share to a private cloud, the App Controller machine account needs read access to the file share.

To copy resources from a private cloud to a network file share, the App Controller machine account needs write access to the file share.

See Also

Using App Controller Library Resources

How to Add or Remove File Shares in the App Controller Library

Adding a File Share to the App Controller Library

Administrators can add file shares to the App Controller Library. Share access control is managed by the file server. Administrators should verify that users have the appropriate access to a share before adding it to the App Controller Library.

To add a file share to the App Controller Library

1. On the **Library** page, click **Shares**.
2. Click **Add Share**.
3. In the **Add a network shared folder** dialog box, enter the share path.
4. Click **OK**.

> **Note**
> If files will be copied to this share from a VMM cloud library, or from this share to a VMM cloud library, the App Controller machine account must be added to the file share permission list.

Removing a File Share from the App Controller Library

Administrators can remove file shares no longer needed from the App Controller Library.

To remove a file share from the App Controller Library

1. On the **Library** page, click **Shares**.
2. In the right pane, select the share to be removed.
3. Select **Remove Share**.

See Also

Using App Controller Library Resources

How to Add or Remove a Windows Azure Storage Account

Users can add or remove Windows Azure storage accounts if they have access to the Windows Azure subscription.

To add a Windows Azure storage account

1. On the **Library** page, expand the **Windows Azure** node.
2. Expand the **Windows Azure** subscription in which the new storage account should be created.
3. Click **Create Storage Account** in the taskbar.

4. In the **Create Storage Account** dialog box, enter the new account name.

   Note
   The storage account name must be between 3 and 24 characters in length and use lower-case letters and numbers only.

5. Select a geographical region or affinity group for the new storage account and then click **OK**.

To delete a Windows Azure storage account

1. On the **Library** page, expand **Windows Azure**.
2. Expand the **Windows Azure** subscription from which the existing storage account should be removed.
3. Click **Delete**.
4. Click **Yes** to delete the storage account.

See Also

How to Add or Remove a Windows Azure Storage Container

Using App Controller Library Resources

How to Add or Remove a Windows Azure Storage Container

Add a Windows Azure Storage Container

Users can add a Windows Azure storage container if they have access to the Windows Azure subscription.

To add a Windows Azure storage container

1. On the **Library** page, expand the **Windows Azure** node.
2. Expand the **Windows Azure** subscription in which the new container should be created.
3. Select the **Windows Azure** storage account in which the new container should be created.
4. Click **Create Container**.
5. In the **Create Container** dialog box, enter the new container name. The container name must be a valid DNS name. For more information about naming containers, see Naming and Referencing Containers, Blobs, and Metadata.
6. Click **OK**.

Delete a Windows Azure Storage Container

Users can remove a Windows Azure storage container if they have access to the Windows Azure subscription.

To delete a Windows Azure storage container

1. On the **Library** page, expand **Windows Azure**.
2. Expand the **Windows Azure** subscription from which the existing container should be removed.
3. Select the **Windows Azure** storage account from which the existing container should be removed, then select the container.
4. Click **Delete**.
5. Click **Yes** in the **Confirm delete** dialog box.

See Also

How to Add or Remove a Windows Azure Storage Account

Using App Controller Library Resources

How to Copy Files from Shares to Public Clouds

Copying Files from Shares to Windows Azure Storage

Authorized users can copy files from shares to their corresponding public cloud libraries.

To copy files from a share to Windows Azure

1. Go to the **Library** page and navigate to the share from which files should be copied.
2. Select the file or files to be copied.
3. Click **Copy**.
4. Navigate to the **Windows Azure** storage container.
5. Click **Paste**.

Copying VHD Files from a Share to a Windows Azure Container

Authorized users can copy VHD files from shares to their corresponding Windows Azure image container. The container contains virtual hard disk files used by the **VMRole** in Windows Azure. Only .vhd files can be copied to the image container.

To copy VHD files from shares to a Windows Azure container

1. Go to the **Library** page and navigate to the share from which files should be copied.
2. Navigate to the directory from which files should be copied.
3. Select a single file with a .vhd file name extension.
4. Click **Copy**.
5. Navigate to the Windows Azure container.
6. Click **Paste**.

7. In the **Copy a virtual hard disk** dialog, enter a new name if necessary.
8. If the disk is a base disk, select a region or affinity group. If the disk is a differencing disk, click **Select** to select the parent disk. Note the differencing disk will be placed at the same region or affinity group of the parent disk.
9. Click **OK**.

See Also

How to Copy Files from Shares to Private Clouds

How to Copy Library Resources Between Clouds of the Same Type

How to Add or Remove File Shares in the App Controller Library

Using App Controller Library Resources

How to Copy Files from Shares to Private Clouds

Copying Files from a Share to Private Cloud Libraries

VMM Administrators can copy files from local shares to any VMM cloud library. VMM users can copy files from local shares to folders in private cloud libraries.

To copy files from shares to a VMM cloud library

1. Go to the **Library** page and navigate to the share from which files should be copied.
2. Navigate to the directory from which files should be copied.
3. Select file or files to be copied.
4. Click **Copy**.
5. Navigate to the VMM Cloud Library.
6. Click **Paste**.

See Also

How to Copy Files from Shares to Public Clouds

How to Copy Library Resources Between Clouds of the Same Type

How to Add or Remove File Shares in the App Controller Library

Using App Controller Library Resources

How to Copy Library Resources Between Clouds of the Same Type

Copying Resources Between Two Windows Azure Subscriptions

Resources can be copied between Windows Azure subscriptions.

To copy resources from one Windows Azure subscription to another

1. Go to the **Library** page and navigate to the Windows Azure storage container from which the files should be copied.
2. Select files to be copied and click **Copy**.
3. Navigate to the destination Windows Azure storage container.
4. Click **Paste**.

Copying VMM Templates Between Two VMM Servers

VMM virtual machine templates or service templates can be copied between two VMM servers. VMM Administrators can select any destination VMM cloud library. VMM self-service users can select their corresponding folders in private cloud libraries.

To copy a VMM template between two VMM servers

1. Go to the **Library** page and navigate to the VMM template node from which a virtual machine template or service template should be copied.
2. Select the template you want to copy and click **Copy**.
3. Navigate to the destination VMM cloud library share.
4. Click **Paste**.
5. In the **Copy Template** dialog box, for each dependent resource of the template, select either **copy to destination** or **map to existing**.
6. Click **OK**.

> **Note**
> If files are copied to destination VMM cloud libraries, temporary storage is needed. By default, the temporary storage location is on the App Controller server under **%programdata%\Microsoft\System Center\App Controller**. It can be updated to a network share using the PowerShell cmdlet **Set-SCACTemporaryStorage**. The App Controller computer account must be added to the network share permission list.

See Also

Using App Controller Library Resources

How to Deploy a Virtual Machine Template to a Private Cloud

To deploy a virtual machine template to a private cloud

1. Go to the **Library** page and navigate to the VMM server in which the template is stored.
2. Expand the **Templates** node and then select the template to be deployed.

3. Click **Deploy** in the taskbar.
4. In the **Select a cloud for this deployment** dialog box, select the cloud to deploy the template to and then click **OK**.
5. In the **New Deployment** dialog box, configure the new virtual machine or service.
6. Click **Deploy**.

See Also

Deploying Services and Virtual Machines

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

How to Refresh VMM Library Server Certificates

When a new library server is added to a VMM server, new SSL certificates need to be imported to allow file copying to and from the new library share.

To refresh VMM server certificates

1. In the App Controller console, expand the **Settings** node.
2. Click **Connections**.
3. Select the VMM server with the new library share from the list view.
4. Click **Refresh Certificates** in the taskbar.

Note
In order for the refresh to succeed, users need to be part of all of the following roles: the local administrator of the App Controller server, local administrator of the VMM server, and VMM administrator.

See Also

Using App Controller Library Resources

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

Before you begin this task:

1. If you are uploading from a file share or from a VMM library, ensure that you have a destination storage container prepared in Windows Azure.
2. If you are uploading a virtual hard disk, verify the operating system (if any) that is installed on the disk before you proceed.

To upload a virtual hard disk or image to Windows Azure

1. On the **Library** page, expand the **Windows Azure** node.
2. Expand the Windows Azure subscription to the Windows Azure storage account in which the destination container is located.

3. Do one of the following:
   - To upload a virtual hard disk, select the **Disks** folder and click **Add** in the taskbar.
   - To upload an image, right-click the **Images** folder and click **Add** in the taskbar.
4. Specify the file share, VMMlibrary, or Windows Azure storage container from which you want to retrieve the source disk or image.
5. Do one of the following:
   - For a virtual hard disk, specify the operating system that is installed on the disk. If no operating system installed, select **None**.
   - For a disk image, specify the operating system that is installed on the image.
6. Click **OK**.

See Also

How to Add or Remove a Windows Azure Storage Account

Using App Controller Library Resources

Setting up Public and Private Clouds

Use System Center 2012 - App Controller to connect to and manage public and private clouds, and to deploy services to them. Users who manage public and private clouds must be members of the **Administrator** user role. For more information about user roles, see Managing User Roles.

Important
In this release of App Controller, you can only connect to Windows Azure subscriptions (public clouds) and System Center 2012 – Virtual Machine Manager (VMM) clouds.

In App Controller, the **Clouds** page displays the following information:

- A list of all public and private clouds, further grouped by connection name.
- The properties of each public and private cloud to which App Controller is connected.
- Resources used and available on private clouds.
- Tasks you can perform on a selected public or private cloud.

Information on the clouds page can be viewed as a list, or as tiles. Use the tile and list icons on the taskbar to switch between card and list.

In This Section

How to Connect to Public Clouds

Describes how to connect a Windows Azure subscription to App Controller.

How to Connect to Private Clouds

Describes how to connect a System Center 2012 – Virtual Machine Manager (VMM) management server to App Controller.

How to Connect to a Hosting Provider in System Center 2012 SP1

Describes how to connect a hosting service provider to App Controller.

How to Remove a Connection to a Public Cloud

Describes how to remove a Windows Azure subscription in App Controller.

How to Remove a Connection to a Private Cloud

Describes how to remove a VMM server in App Controller.

How to Remove Certificates for VMM Library Servers

Describes how to remove SSL certificates associated with VMM library servers.

How to Delegate Users

Describes how to create a App Controller user role profile and define which users to add as members of this user role.

How to View or Change Run As Accounts

Describes how to create, edit or delete Run As accounts on private clouds.

How to View or Change Public Cloud Properties

Describes how to view or change the properties of a public cloud.

How to View or Change Private Cloud Properties

Describes how to view or change the properties of a private cloud.

How to View Public or Private Cloud Usage

Describes how to view public and private cloud usage information.

How to View or Change Cloud Services and Certificates

Describes how to view or change the properties of a public or private cloud.

Managing Windows Azure Subscription Settings

Describes how to manage Windows Azure subscription settings.

Managing Connection Settings

Describes how to manage public and private cloud connection settings.

How to View the Status of a Job

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

Related Sections

Getting Started with System Center 2012 - App Controller

Deploying Services and Virtual Machines

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

Using the Windows PowerShell module for App Controller

How to Connect to Public Clouds

Connecting a Windows Azure Subscription to App Controller

Certificates are used to set up trust between the Windows Azure management API and App Controller. This authentication allows App Controller to call on the Windows Azure API when you perform tasks such as deploying services or change configuration properties. The service certificate, or Personal Information Exchange certificate (.pfx file), contains a private key. App Controller stores this certificate in the App Controller database. Since the certificate contains the private key, you need to provide the password so that App Controller can use the private key. The management certificate (.cer file) contains only the public key, which is kept in Windows Azure for accessing the API. Windows Azure allows customers to create their own management certificates, either self-signed certificates or using their preferred certification authority (CA). By giving Windows Azure the public key and keeping the private key local, the authentication can be completed.

If you are creating a certificate, you will need to export the certificate twice—once as a .cer file, and then a second time as a .pfx file, for use in App Controller. For more information about how to create and export certificates for connections to Windows Azure subscriptions, see How to Create a Management Certificate and How to Add a Management Certificate to a Windows Azure Subscription in the Windows Azure Platform section of the MSDN Library.

You may need to configure proxy configuration settings before adding subscriptions. For information on proxy configuration, see Managing Connection Settings.

Important

You must be a member of the App Controller Administrator user role in order to perform the following procedures. For more information about user roles, see Managing User Roles.

To connect App Controller to a Windows Azure subscription

1. On the **Clouds** page, click **Connect** and then click **Windows Azure Subscription**.
2. In the **Connect** dialog box, enter a name for this subscription. This name is displayed in the **Name** column of the **Clouds** page.
3. Add an optional description in the **Description** text box.
4. In the **Subscription ID** field, enter the subscription ID for this connection. The Windows Azure subscription ID is a GUID and can be found in the Windows Azure Management Portal.
5. To import the required management certificate, select the Personal Information Exchange (.pfx) file for the public key you uploaded to Windows Azure and enter the password for the certificate.
6. Click **OK** to create the connection.

Tip

When you add a Windows Azure subscription, it might take some time for tasks related to that subscription to be displayed as available. To quickly refresh the view, close the App Controller browser windows, and connect again to the App Controller site.

See Also

How to Refresh VMM Library Server Certificates

How to View the Status of a Job

Managing Connection Settings

Managing Windows Azure Subscription Settings

How to Connect to Private Clouds

How to Connect to Private Clouds

Connecting a System Center 2012 – Virtual Machine Manager (VMM) Server to App Controller

To connect App Controller to a VMM server

1. On the **Clouds** page, click **Connect** and then click **VMM Server**.
2. In the **Connect** dialog box, enter a name for this connection. This name is displayed in the **Name** column of **Clouds** page.
3. Add an optional description in the **Description** text box.
4. In the **Server name** text box, enter the fully qualified domain name (FQDN) of the

VMM management server.

5. In the **Port** field, enter a port number that matches the port used by the VMM management server (default: 8100).
6. Check **Automatically import SSL certificates** if you plan to copy files and templates to and from VMM cloud libraries.

   Note
   SSL certificates must be imported to the App Controller server in order to copy files or templates to and from VMM cloud libraries. In order for the import to succeed, users need to be part of all of the following roles: the local administrator of the App Controller server, local administrator of the VMM server, and VMM administrator.
7. Click **OK** to create the connection.

   You may then be asked to select which VMM user role to use from the new VMM server connection for the current session.

See Also

How to Refresh VMM Library Server Certificates

How to View the Status of a Job

Managing Connection Settings

Managing Windows Azure Subscription Settings

How to Connect to Public Clouds

How to Connect to a Hosting Provider in System Center 2012 SP1

Connecting a Hosting Provider to App Controller

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

Certificates are used to set up trust between the Service Provider Foundation and App Controller. This authentication allows App Controller to call on the Service Provider Foundation when you perform tasks such as deploying services or changing configuration properties. The tenant certificate, or Personal Information Exchange certificate (.pfx file), contains a private key. App Controller stores this certificate in the App Controller database. Since the certificate contains the private key, you need to provide the password so that App Controller can use the private key. The tenant certificate (.cer file) in the Service Provider Foundation that corresponds to the tenant certificate in App Controller contains only the public key, which is kept in the Service Provider Foundation for access. The Service Provider Foundation allows customers to create their own management certificates, either self-signed certificates or using their preferred certification authority (CA). By giving the Service Provider Foundation the public key and keeping the private key local, the authentication can be completed.

If you are creating a certificate, you will need to export the certificate twice—once as a .cer file, and then a second time as a .pfx file, for use in App Controller. You may need to configure proxy configuration settings before adding subscriptions. For information on proxy configuration, see Managing Connection Settings.

Important

The tenant certificate in the Service Provider Foundation must be validated by the App Controller server. Ensure that the certificate is:

- Not expired.
- Issued by a trusted certification authority (CA). However, if you are testing with a self-issued certificate created by IIS, you must add the certificate to the Trusted Root Certification Authorities store of the local machine account.
- The common name (CN) that is used in the Subject attribute of the certificate must match the tenant ID. However, if you are testing this feature, you can disable validation by adding the following code snippet to *install_folder*\api\bin\Microsoft.SystemCenter.CloudManager.Providers.SpfVmm.exe.config:

```
    <system.net>
      <settings>
        <httpListener unescapeRequestUrl="false"/>
        <servicePointManager checkCertificateName="false"
checkCertificateRevocationList="false" />
      </settings>
    </system.net>
```

To connect App Controller to a hosting provider

1. On the **Settings** page, expand **Connections** in the navigation pane, click **Connect** and then click **SPF**.
2. In the **Add an external service provider connection** dialog box, enter a name that you can use to identify this hosting provider connection. This name will be displayed in the **Connection Name** column of the **Clouds** page.
3. Add an optional description in the **Description** text box.
4. In the **Service location** box, enter the Service Provider Foundation OData protocol URI for the VMM service, as shown the following example. The URI ends with the tenant ID:

   `http://adatum.contoso.com:8090/SC2012/vmm/Microsoft.Management.Odata.svc/4ce5713a-50a1-434b-b47a-87caad75ba72`
5. To import the required management certificate, select the Personal Information Exchange (.pfx) file that you provided to the hosting service provider and enter the password for the certificate.
6. Click **OK** to create the connection.

See Also

How to Deploy a Virtual Machine

How to Remove a Connection to a Public Cloud

When you remove a connection to a public or private cloud in App Controller, services, virtual machines, and library resources associated with those clouds will no longer be visible in the App Controller console. Those objects will not be deleted by removing a connection to a public or private cloud.

Tip

When you remove a Windows Azure subscription, it might take some time for tasks related to that subscription to be displayed as unavailable. To quickly refresh the view, close the App Controller browser windows, and connect again to the App Controller site.

To remove a connection to a Windows Azure subscription

1. In the navigation pane, click **Settings** and then click **Subscriptions**.
2. In the list of Windows Azure subscriptions, select the subscription you want to remove and then click **Remove**.
3. Click **OK** to remove the selected subscription.

See Also

Managing Connection Settings

Managing Windows Azure Subscription Settings

How to View or Change Cloud Services and Certificates

How to Remove a Connection to a Private Cloud

How to Remove a Connection to a Private Cloud

When you remove a connection to a public or private cloud in App Controller, services, virtual machines, and library resources associated with those clouds will no longer be visible in the App Controller console. Those objects will not be deleted by removing a connection to a public or private cloud.

To remove a connection to a VMM management server

1. In the navigation pane, click **Settings** and then click **Connections**.
2. In the list of VMM management server connections, select the connection you want to remove, and then click **Remove**.
3. Click **OK** to remove the selected connection.

Note

If any SSL certificates are associated with this connection, they must be

manually removed. For more information about removing certificates, see How to Remove Certificates for VMM Library Servers.

See Also

Managing Connection Settings

Managing Windows Azure Subscription Settings

How to View or Change Cloud Services and Certificates

How to Remove a Connection to a Public Cloud

How to Remove Certificates for VMM Library Servers

To remove certificates for VMM library servers

1. On the App Controller server, open the Certificate Manager MMC (certmgr.msc).
2. Open the **Trusted People** store.
3. Delete the certificates for the VMM servers that are no longer needed.

Note
Certificates will have a friendly name that starts with **SCVMM_CERTIFICATE_KEY_CONTAINER**.

See Also

How to Remove a Connection to a Public Cloud

How to Delegate Users

Delegating Users' Access to Private Clouds

Use the System Center 2012 – Virtual Machine Manager (VMM) console to provide users with access to VMM clouds.

Delegating Users' Access to Public Clouds

Before you can assign a user access to a Windows Azure subscription, you must first create a user role so you can add the user as a member of that role. A user role defines which permissions a specified group of users has to public clouds. For more information about user roles, see Managing User Roles.

If you have not yet created a user role, follow the steps in How to Create a User Role in App Controller. This topic also includes the steps required to delegate a user access to a Windows Azure subscription.

Delegating Users' Access to Hosting Service Providers

For System Center 2012 SP1 only: Before you can assign a user access to a hosting service provider, you must first create a user role so you can add the user as a member of that role. A user role defines which permissions a specified group of users has to public clouds. For more information about user roles, see Managing User Roles.

If you have not yet created a user role, follow the steps in How to Create a User Role in App Controller. This topic also includes the steps required to delegate a user access to a hosting service provider.

See Also

How to Create a User Role in App Controller

Managing User Roles

How to View or Change Run As Accounts

To view or change Run As accounts on a private cloud

1. In the navigation pane, click **Clouds**. Select a private cloud from the list and then click **Manage Run As Accounts** in the taskbar.
2. Click **New** to add an account.
3. Select an account from the list and click **Edit** to change the account.
4. Select an account from the list and click **Delete** to remove the account. A Run As account can only be deleted by the user who created the Run As account.

   Note
   To share a Run As Account with other users, it is necessary to use either Windows PowerShell or the VMM console to add permissions to the Run As account.

See Also

Setting up Public and Private Clouds

How to View or Change Public Cloud Properties

The following section describes the Windows Azure subscription properties that can be changed in App Controller. To view or change the connection properties of a private or public cloud, see Managing Connection Settings.

Configuring Windows Azure Subscription Properties

After you connect to a Windows Azure subscription in App Controller, you can make changes to the following properties:

- **Name**—a display name that you can create to identify this subscription. This name will be displayed on the **Clouds** page in the **Clouds** column of the list view.
- **Description**—an optional description you can use to provide more information about the subscription.
- **Subscription ID**—a Windows Azure subscription ID, obtained from the Windows Azure Management Portal. This value cannot be changed after it has been added.
- **Management certificate**—an X.509 v3 certificate used to authenticate App Controller with Windows Azure to manage subscription resources.
- **Management certificate password**—the password created for use with the Management certificate.

Note
For more information about how to create and export certificates for connections to Windows Azure subscriptions, see How to Connect to Public Clouds.

To change Windows Azure subscription properties

1. On the **Clouds** page, select the Windows Azure subscription you want to change and then click **Properties** in the taskbar.

   Tip
   You can also click **Subscriptions** under the **Settings** node of the navigation pane to change Windows Azure subscription properties. For more information about changing these settings from the Settings node, see Managing Windows Azure Subscription Settings.
2. In the **Name** text box, enter a new display name for this subscription.
3. In the **Description** text box, enter an optional description.
4. To import the management certificate, browse for and then select the Personal Information Exchange (.pfx) certificate.
5. In the **Management certificate password** text box, enter the password for the certificate you selected in the previous step.
6. Click **OK** to save your changes.

See Also

Managing Connection Settings

How to View or Change Private Cloud Properties

How to View or Change Private Cloud Properties

The following section describes how to change private cloud properties in App Controller.

To Configure Private Cloud Properties

1. To change the connection name and description for a private cloud, proceed as

described in Managing Connection Settings.

2. To perform other operations on VMM clouds, use the System Center 2012 – Virtual Machine Manager (VMM) console.

See Also

How to View or Change Public Cloud Properties

How to View Public or Private Cloud Usage

Switching to the card view allows you to view the usage of private and public clouds.

To view public and private cloud usage

1. Click the **Clouds** node.
2. If a list of clouds is displayed, click the toolbar icon to switch to the card view. The tooltip is “Show items as cards.” For each cloud, the following usage information is displayed.
   - **Private Clouds**—Displays the number of services running in each private cloud, and also the number of resources used and available for the following resources:
     - Virtual machines
     - Processors
     - Memory
     - Storage
   - **Public Clouds**—Displays the number of deployed services in each Windows Azure subscription and will identify if any services are currently stopped, or if a service has only one instance running. Stopped services continue to accrue charges while services with only one instance are not covered with the Windows Azure compute Service Level Agreement (SLA).

See Also

Overview of the App Controller Console

Managing Windows Azure Subscription Settings

Managing Connection Settings

How to View or Change Cloud Services and Certificates

The following section describes how to view, add, and delete cloud services in a Windows Azure subscription, as well as how to manage certificates for a cloud service.

Note

A cloud service is a container for your service deployments in Windows Azure. Your subscription may have a limit on the number of cloud services that can be created. If you

reach this limit you will not be able to create a cloud service until an existing cloud service is deleted.

For System Center 2012 SP1 only: For information managing certificates for a connection to a hosting service provider, see How to Connect to a Hosting Provider in System Center 2012 SP1.

To add or delete a certificate to a cloud service

1. From the **Clouds** page, select a Windows Azure subscription from the list and click **Manage Cloud services** in the task bar.
2. Select a cloud service from the list and click **Certificates**.
3. To add a certificate to the cloud service, click **Add Certificate**.

   The certificate must be in either a Windows Azure storage account or on a network file share that is already added to App Controller. The certificate is a PFX file, and to access the file you will need to enter the password used to protect the PFX file. When you add a certificate to a cloud service, the certificate is uploaded to the certificate store of the Windows Azure subscription.
4. To delete a certificate from the cloud service, select the certificate you want to delete and click **Remove Certificate**.

   When you delete a certificate, the certificate is deleted from the certificate store of the Windows Azure subscription and will no longer be available for use by services deployed in the subscription.

To create a new cloud service

1. From the **Clouds** page, select a Windows Azure subscription from the list and click **Manage Cloud services** in the task bar.
2. Click **Create** to create a new cloud service.
3. Enter a name for the cloud service and an optional description.
4. Enter a public URL for the cloud service.

   Note
   The public URL you give the new cloud service must be unique across Windows Azure.
5. Select a region in which to deploy the new cloud service.

   Note
   When you create a cloud service, you must specify a geographical location for it. You can do this either by specifying a geographic location or by specifying that the service should be part of an affinity group.

To delete a cloud service

1. From the **Clouds** page, select a Windows Azure subscription from the list and click **Manage Cloud services** in the task bar.

2. Select the cloud service you want to delete from the list and then click **Delete**.

   A cloud service can only be deleted if there are no services deployed to the cloud service. If a cloud service has certificates, the certificates will be deleted from the certificate store when the cloud service is deleted.

   Note

   If you are creating a new cloud service, the public URI that you give your cloud service must be unique across Windows Azure. When you create a cloud service, you must specify a geographical location for it. You can do this either by specifying a data geographic location or by specifying that the service should be part of an affinity group. Additionally, you can upload certificates for use of deployments in the cloud service. Certificates can be used by a service for many purposes including SSL for a web role or encrypting remote desktop passwords.

See Also

Deploying Services and Virtual Machines

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

Setting up Public and Private Clouds

Managing Windows Azure Subscription Settings

In order to add a Windows Azure subscription, you first need to create and export a Personal Information Exchange certificate (.pfx). This certificate is used as a service certificate and is needed for creating a remote desktop connection. For more information about how to create and export certificates for connections to Windows Azure subscriptions, see How to Connect to Public Clouds.

When you remove a Windows Azure subscription, services and library resources associated with that public cloud will no longer be visible in the App Controller console; however they will not be removed from the associated Windows Azure subscription.

To add a Windows Azure subscription to App Controller

1. In the **Settings** node, select **Subscriptions** and then click **Add**.
2. In the **Name** field, enter a name for this subscription. This name is displayed in the **Name** column of the **Subscriptions** page.
3. Add an optional description in the **Description** text box.
4. In the **Subscription ID** field, enter the subscription ID for this connection. Windows Azure subscription IDs can be found in the Windows Azure Management Portal.
5. To import the required management certificate, select the Personal Information Exchange (.pfx) file you previously exported and enter the password you created for that certificate.
6. Click **OK** to add the subscription.

To change Windows Azure subscription properties

1. Click **Subscriptions** under the **Settings** node of the navigation pane, select the Windows Azure subscription you want to change and then click **Properties** in the taskbar.
2. In the **Name** text box, change the display name for this subscription.
3. In the **Description** text box, enter or change the optional description.
4. To change the management certificate, browse for and then select the Personal Information Exchange (.pfx) certificate to import it.
5. In the **Management certificate password** text box, enter the password for the certificate you selected in the previous step.
6. Click **OK** to save your changes.

To remove a Windows Azure subscription

1. In the **Settings** node, click **Subscriptions**.
2. In the list of Windows Azure subscriptions, select the subscription you want to remove and then click **Remove**.
3. Click **OK** to remove the selected subscription.

See Also

How to Connect to Public Clouds

How to View or Change Public Cloud Properties

How to Remove a Connection to a Public Cloud

Managing Connection Settings

Configuring Windows Azure Subscription Connection Properties

You can make changes to the following properties of the Windows Azure connection:

- **Proxy settings**—the fully qualified domain name (FQDN) and port number of a proxy server, if required, for network access.
- **Proxy server credentials**—the user name and password, if required, for the proxy server.

To change the properties of a Windows Azure subscription connection

1. In the **Settings** node, click **Connections**, select the Windows Azure connection you want to change, and then click **Properties**.
2. In the **Proxy settings** text box, enter the address and port number of your proxy server.
3. If credentials are required to use the proxy server, check **This proxy server requires credentials** and enter the user name and password associated with the proxy server.
4. Click **OK** to save your changes.

Configuring VMM Management Server Connection Properties

After you connect to a VMM management server in App Controller, you can make changes to the following properties:

- **Connection name**—a display name that you can use to identify this connection.
- **Description**—an optional description you can use to provide more information about the connection.

To change the properties of a Virtual Machine Manager for System Center 2012 server connection

1. In the **Settings** node, select **Connections**, select the VMM connection you want to change, and then click **Properties**.
2. In the **Connection name** text box, change the name you want to use to identify this connection.
3. In the **Description** text box, enter an optional description for this connection.
4. Click **OK** to save your changes.

See Also

Managing Windows Azure Subscription Settings

How to Connect to Public Clouds

How to View or Change Public Cloud Properties

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 Install a Language Pack

To install a language pack

1. In the LanguagePack folder on your App Controller installation media, right-click **ACLanguagePack.msi**, and then click **Run as administrator**.
2. Review the license terms, select the **I accept the terms in the License Agreement** check box, and then click **Install**.
3. After setup is complete, click **Finish**.

To uninstall a language pack

1. On the computer on which the App Controller server is installed, click **Start**, and then

click **Control Panel**.

2. Under **Programs**, click **Uninstall a program**.
3. Under **Name**, double-click **Language Pack for App Controller**.
4. Click **Yes** in the confirmation dialog box.

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

Getting Started with System Center 2012 - App Controller

Setting up Public and Private Clouds

Deploying Services and Virtual Machines

Using the Windows PowerShell module for App Controller

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

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

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 or Private 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

Troubleshooting System Center 2012 - App Controller

We recommend that you only perform diagnostic tracing in association with a Microsoft Customer Support Services (CSS) representative when troubleshooting issues with System Center 2012 - App Controller. We recommend this because the trace information generated contains information about the context of a text-based trace message. This text contains only low-level information such as source code file names, locations, source code functions, and return codes. This information may be helpful if you have to troubleshoot a complex issue.

Troubleshooting Client Connections

If you use a self-signed certificate, the certificate must be added to the Trusted Root Certification Authorities store of all computers that will access the App Controller website. Some browsers will fail to display App Controller after the login screen if the certificate is not trusted.

Troubleshooting Job Failures

Many activities result in the creation of a job. If a job fails, the error details provide additional information that can be used to understand the cause of the failure.

Adding a Windows Azure Subscription

Error message: The certificate is not valid or the password is incorrect.

Resolution: Confirm that the certificate file is identified in Windows Explorer as a Personal Information Exchange (.pfx) file. Ensure the password being used is the same password that was specified when creating or exporting the certificate.

To validate the certificate and password outside of App Controller, import the certificate into the local certificate store using the Certificate Import Wizard in Windows. Right-click the .pfx file and select **Install PFX** to start the import process.

In addition, validate that your proxy settings, if required for the Windows Azure connection, are correct.

Error message: The server failed to authenticate the request. Verify that the certificate is valid and is associated with this subscription. Error code from Windows Azure: AuthenticationFailed.

Resolution: Upload the certificate to Windows Azure using the Windows Azure Management Portal. See How to Connect to Public Clouds for more information about how to connect a Windows Azure subscription to App Controller.

Deploying a Windows Azure Service

Error message: One or more configuration settings are specified for this deployment configuration but are not defined in the service definition file: [filename].

Resolution: This may be the result of the service configuration file and the package file not matching. Review the command parameters of the job details to identify the package used.

Copying Files to a Private Cloud

The computer account of the App Controller server needs read access to the enterprise share to be able to copy files from an enterprise share.

The computer account of the App Controller server needs write access to the enterprise share to be able to copy files to an enterprise share.

Client Diagnostics

Each client automatically maintains a history of diagnostic information. This diagnostic information is stored in memory and a set number of diagnostic entries are saved. When the limit of entries is reached, the oldest entry is deleted to allow the new entry to be written. The diagnostic information is automatically cleared when the client exits, as part of closing the browser or refreshing the browser window.

Configuring Collection of Diagnostic Information

By default, the client will only record errors and warnings up to 500 entries. You can increase or decrease the amount diagnostic information recorded, along with how much history is kept, in the logging options window. To access the logging options, press **CTRL+ALT+SHIFT+L**.

- If you a signed in as an Administrator you can also access the logging options by clicking on the icon next to the last refresh time in the toolbar of the **Overview** page.
- To increase or decrease the types of information recorded, check or clear the boxes on this screen.
- To increase or decrease the amount of information recorded, specify the number of lines of information to be recorded. Increasing the number of lines will increase the memory used by the client.

Saving and Viewing Diagnostic Information

To save or view the diagnostic information, open the logging options window. To access the logging options, press **CTRL+ALT+SHIFT+L**.

- If you a signed in as an Administrator you can also access the logging options by clicking on the icon next to the last refresh time in the toolbar of the Overview page.
- On this page you can choose to copy the log to the clipboard or save the diagnostics to a file. If you copy the diagnostics to the clipboard, you can paste the information into an application such as Notepad to view, or into an e-mail to send to your support engineer.

Server Diagnostics

To enable diagnostic information from the server, collect traces information by using the debug view, as shown in the following procedure.

- Open a command prompt as Administrator.
- Go to the **%programfiles%\Microsoft System Center 2012\App Controller\Tracing** folder.
- To start tracing, run **starttracing.cmd VER** at the command prompt.

  Note
  Possible trace levels are WRN, INF, ERR and VER, which correspond to Warning, Informational, Error and Verbose. For troubleshooting, we recommend that you use the VER trace level.
- Reproduce the issue.
- Run **stoptracing.cmd**.
- Run **formattracing.cmd –DebugViewFormat**, which formats the tracing data so that it is readable. This command displays the folder name to which the trace files get saved. Open the folder, and then copy the files to share them with Microsoft Customer Support Services..

See Also

How to View the Status of a Job

How to Connect to Public Clouds

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 as CPUs, memory, storage, virtual machines, and so on.
scope	The set of public and private clouds to which a user role has access.

Term	Definition
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 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

Term	Definition
	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.

Release Notes for System Center 2012 - App Controller

The following release notes apply to the appropriate version of App Controller in System Center 2012, and they contain descriptions and workarounds for known issues.

There are three versions of these release notes:

1. Release Notes for System Center 2012 - App Controller
2. Release Notes for App Controller in System Center 2012 SP1
3. **Release Notes for App Controller in System Center 2012 R2**

See Also

App Controller

Release Notes for System Center 2012 - App Controller

These release notes contain information that is required to successfully install System Center 2012 - App Controller. They contain information that is not available in the product documentation.

Before you install and use App Controller, read these release notes. These release notes apply to System Center 2012 - App Controller.

If you are looking for the Release Notes for App Controller in System Center 2012 Service Pack 1 (SP1), see **Release Notes for App Controller in System Center 2012 Service Pack 1**.

Known Issues

App Controller cannot share SQL Server instance

Description: You receive the following error when specifying a SQL Server instance that previously contained an App Controller database: **App Controller SQL Agent jobs installed. App Controller cannot share SQL Server instance**.

Cause: Previous builds of App Controller did not correctly remove the SQL Server Agent Jobs when removing the database.

Workaround: Manually remove the two SQL Server Agent jobs that begin with **CloudManager**, and then attempt App Controller Setup again.

App Controller appears to stop responding when checking for updates

Description: Setup appears to “hang” or stop responding when checking for updates after clicking **Install** on the first screen of setup.

Cause: App Controller is unable to check for updates on Microsoft Update and takes around 7-10 minutes before returning to setup.

Workaround: Ensure there is connectivity to the Internet when checking for updates. For additional troubleshooting information, see Microsoft Knowledge Base article 836941 (http://go.microsoft.com/fwlink/?LinkId=232284.

Error when running Setup after an uninstall

Description: If you run Setup after uninstalling App Controller on the same computer, you might see Setup return an error.

Cause: After uninstalling App Controller, a race condition can occur with configuring the IIS website.

Workaround: After uninstalling App Controller, restart the computer before you run Setup again.

Cannot connect to App Controller after running Setup

Description: Cannot navigate to App Controller after installing.

Cause: The SSL certificate that was specified during Setup was not valid.

Workaround: Use the IIS Management Console to change the SSL certificate used by App Controller.

Certain characters cannot be used in VMM user role names

Description: An error is reported when using certain characters in a VMM user role name with App Controller.

Cause: App Controller does not support VMM user role names that end with '.' or contain '+'.

Workaround: App Controller can be configured to support '+' in user role names. For more information, see the article at Microsoft Support.

Overlapping tooltips and error messages

Description: Tooltips and error messages can overlap text fields when using a high DPI setting, or a browser zoom other than 100%.

Cause: Incorrect calculation of the location to display the tooltip or error message.

Workaround: Change the browser zoom or DPI setting.

No keyboard input during console connection

Description: Console session for virtual machine does not accept keyboard input.

Cause: Virtual machine has lost keyboard focus.

Workaround: Click the **Reconnect** button to regain keyboard focus for virtual machine.

Keyboard navigation issues

Description: Difficulty using only the keyboard to navigate.

Cause: Keyboard focus is not always clearly shown.

Workaround: Use a mouse or other pointing device.

Changing ownership of virtual machine

Description: A member of a self-service user role is unable to change the ownership of a virtual machine to another user.

Workaround: Have an App Controller Administrator change ownership of the virtual machine.

Windows Azure .cscfg files created in App Controller might not work as expected

Description: Any .cscfg files created by a prerelease version of App Controller might not work correctly when used in a region other than the one for which it was created, because the expiration date might be misinterpreted (for example, the month and day transposed) or might not be readable at all.

Cause: App Controller did not store the expiration date in ISO 8601 format (for example, “2008-04-10T06:30:00.0000000-07:00”), but instead stored it in the short date format for the local region (for example, “10/25/2012”).

Workaround: Edit the .cscfg file in a text file editor such as Notepad, and change the Expiration Date to ISO 8601 format or upgrade to the release version of App Controller.

App Controller site might not connect when published

Description: When you publish the App Controller site such that the publishing rule maps the external IP address of the server to the internal site that is part of an isolated domain for App Controller, you might see a security exception.

Cause: When the App Controller site is being downloaded from one site, but Silverlight is trying to send requests to a different site, Silverlight cross-site protection triggers the security exception.

Workaround: Configure a clientaccesspolicy.xml file as described in Making a Service Available Across Domain Boundaries. Place the file in `%programfiles%\System Center 2012\App Controller\wwwroot` and reload the Silverlight client.

Import of VMM library certificates might not succeed

Description: When you access App Controller from a browser that is running on the App Controller server, you might not be able to successfully import VMM library certificates.

Workaround: Import the library certificates from a remote browser session.

Administrators can sign in to App Controller but cannot see settings

Description: Running the Repair option on App Controller from the Programs and Features control panel removes database configuration information for App Controller. Without this configuration information, App Controller services are not able to connect to the database. Administrators can sign in to App Controller but cannot see App Controller settings.

Fix: Download and install App Controller Update Rollup 1 (UR1) from Microsoft Update (available April 10, 2012).

Workaround: If App Controller UR1 is not or cannot be installed, the following changes can be made to restore the database configuration. In the **Microsoft.SystemCenter.CloudManager.Providers.System.exe.config** file, set the connection strings from following:

```
<connectionStrings>

<add name="CloudSystemsContainer" connectionString=""
providerName="System.Data.EntityClient"/>

<add name="AuthorizationEntities" connectionString=""
providerName="System.Data.EntityClient"/>

<add name="JobsDataContext" connectionString=""
providerName="System.Data.EntityClient"/>

</connectionStrings>
```

To the following (where [DATASOURCE] is the SQL Server data source used for the App Controller database (such as localhost\instance1) and [DATABASENAME] is the App Controller database name):

```
<connectionStrings>

<add name="CloudSystemsContainer"
connectionString="metadata=res://Microsoft.SystemCenter.CloudManager.Providers.System/Clo
udSystems.csdl|res://Microsoft.SystemCenter.CloudManager.Providers.System/CloudSystems.ss
dl|res://Microsoft.SystemCenter.CloudManager.Providers.System/CloudSystems.msl;provider=S
```

```
ystem.Data.SqlClient;provider connection string=&amp;quot;Data Source=[DATASOURCE];Initial
Catalog==[DATABASENAME];Integrated Security=True;MultipleActiveResultSets=True;Connect
Timeout=30&amp;quot;" providerName="System.Data.EntityClient"/>

                                <add name="AuthorizationEntities"
connectionString="metadata=res://Microsoft.SystemCenter.CloudManager.Providers.System.Com
mon/Authorization.csdl|res://Microsoft.SystemCenter.CloudManager.Providers.System.Common/
Authorization.ssdl|res://Microsoft.SystemCenter.CloudManager.Providers.System.Common/Auth
orization.msl;provider=System.Data.SqlClient;provider connection string=&amp;quot;Data
Source=[DATASOURCE];Initial Catalog==[DATABASENAME];Integrated
Security=True;MultipleActiveResultSets=True;Connect Timeout=30&amp;quot;"
providerName="System.Data.EntityClient"/>

                                <add name="JobsDataContext"
connectionString="metadata=res://Microsoft.SystemCenter.CloudManager.Providers.JobHandler
/JobsEntityModel.csdl|res://Microsoft.SystemCenter.CloudManager.Providers.JobHandler/Jobs
EntityModel.ssdl|res://Microsoft.SystemCenter.CloudManager.Providers.JobHandler/JobsEntit
yModel.msl;provider=System.Data.SqlClient;provider connection string=&amp;quot;Data
Source=[DATASOURCE];Initial Catalog==[DATABASENAME];Integrated
Security=True;MultipleActiveResultSets=True;Connect Timeout=30&amp;quot;"
providerName="System.Data.EntityClient"/>

                </connectionStrings>
```

Using ENTER to accept characters in the Input Method Editor (IME) clicks the OK button in dialog boxes

Description: When you press the ENTER key to accept characters in the IME, the keypress event is treated as an OK command in App Controller dialog boxes.

Workaround: Use the mouse or the numeric keypad to select IME characters.

See Also

App Controller

Release Notes for App Controller in System Center 2012 SP1

These release notes contain information that is required to successfully install App Controller in System Center 2012 Service Pack 1 (SP1). They contain information that is not available in the product documentation.

Before you install and use App Controller, read these release notes. These release notes apply to App Controller in System Center 2012 SP1.

The information in this topic applies only to System Center 2012 SP1. If you are looking for the Release Notes for the original release of System Center 2012 - App Controller, see Release Notes for System Center 2012 - App Controller.

Known Issues

App Controller Setup does not add all members of local Administrators group to the Administrator user role on Windows Server 2012

Description: The setup does not add all members of the local Administrators group, but it does add the person installing the product as an App Controller Administrator.

Workaround: Manually add the members of the local Administrators group to the Administrator user role in App Controller.

Setup blocks App Controller installation if the IIS prerequisite is not present.

Description: Setup will not allow the user to continue if IIS is not present. This occurs both on Windows Server 2012 and on Windows Server 2008 R2.

Workaround: Install the IIS role on the computer before trying Setup again.

Uninstall will not remove the App Controller database if SQL Server is using the Availability Group feature

Description: Uninstall does not remove the App Controller database.

Cause: SQL Server is using the Availability Group feature.

Workaround: After uninstalling App Controller, remove the database manually.

App Controller Setup crashes when loading prerequisites

Description: Setup crashes when loading prerequisites.

Workaround: Run Setup again without restarting the computer. The problem might return the first time you run Setup after restarting the computer.

If you cancel App Controller upgrade, you cannot uninstall

Description: When you upgrade from a different prerelease version of App Controller to this release, if you cancel the upgrade before it is complete, App Controller cannot be uninstalled; you will see upgrade screens instead of the uninstall screens. Similarly, silent uninstall will also not uninstall the component.

Cause: The files in the App Controller setup folder are replaced by the upgrade files.

Workaround: Successfully complete the upgrade, and then uninstall App Controller.

Unexpected failure possible for App Controller upgrade

Description: Upgrade from the Beta release of App Controller in System Center 2012 SP1 to this release might fail. You will see a red X symbol during the App Controller management server upgrade and a pointer to the Setup logs. The final portion of the Windows Installer log will show a failure to install.

Cause: Unknown.

Workaround: Run Setup again for the upgrade without restarting the computer. Setup should finish successfully, displaying a warning for the management server upgrade warnings. However, despite the warnings, App Controller should be successfully upgraded at this point.

Uploading a file with non-valid characters in the file name to a Windows Azure container will fail

Description: Uploading a file to a Windows Azure container never starts a job, but you are notified that the upload failed.

Cause: There are characters in the file name that are not valid, from among the following: **^%$&)(+!**@#**}{**.

Workaround: Change the file name to eliminate valid characters, and try again.

App Controller header pane containing System Center signout might disappear

Description: The header pane and navigation pane disappear after selecting a few nodes.

Workaround: Enable "Enhanced Security Configuration" settings under Local Computer.

Virtual Machines or templates copied to Windows Azure might remain locked

Description: After an SSU copies a virtual machine or virtual machine template from VMM to Windows Azure, the VMM resource may remain locked, which prevents changes to it. This means a stored virtual machine cannot be moved back to a host.

Workaround: Use the VMM console to cancel the resource Export job that was started by App Controller.

Conflict checks are not performed when you add a data disk with the same name to a virtual machine in Windows Azure using App Controller in System Center 2012 Service Pack 1 (SP1)

Description: When a data disk is being added to a virtual machine in Windows Azure and the virtual machine already has an existing Windows Azure data disk with the same name, the conflict will not be detected in this release of App Controller.

Workaround: None.

A virtual machine in Windows Azure cannot be reimaged using App Controller in System Center 2012 Service Pack 1 (SP1)

Description: Using this release of App Controller, you cannot reimage a virtual machine in Windows Azure either before or after deployment.

Workaround: None.

A deployed service in Windows Azure cannot be upgraded by App Controller in System Center 2012 Service Pack 1 (SP1)

Description: The **Upgrade** command is not available for a deployed service in Windows Azure in this release of App Controller.

Workaround: None.

The Properties command for a virtual machine in Windows Azure does not work in CTP2

Description: In this release of App Controller in System Center 2012 Service Pack 1 (SP1), Windows Azure virtual machine properties cannot be opened. The Properties command in the taskbar does not work and the Properties command on the right-click menu does not work.

Workaround: The virtual machine properties that are available on the **Virtual Machines** page can be viewed.

An Expired or improperly stored certificate can cause an Export job to hang in VMM

Description: If the self-signed certificate used for evaluating App Controller is not stored in the Trusted Root Certification Authorities store on the App Controller management server and on any computer that is accessing App Controller in a browser or running Windows PowerShell commands for App Controller, some features will not work.

- When you copy a virtual machine from VMM to Windows Azure, the export job that copies the VHD will not be allowed to close the export. This will lock up the VHD resource in VMM until someone deletes the job in VMM or the export times out.
- Windows PowerShell commands will not run.
- Firefox cannot be used to access App Controller

Note

These conditions can also be caused by an expired certificate.

Workaround: Manually set up an HTTP binding for evaluation instead of using a self-signed certificate, or ensure that you store the self-signed certificate used for evaluating App Controller in the Trusted Root Certification Authorities store on the computers listed in the description for this release note. Also, ensure that the certificate is not expired.

See Also

App Controller