

Dell Hybrid Cloud System for Microsoft Cloud Platform System (CPS) Standard

Version 1.4 Administrators Guide, based on release 1703

Notes, cautions, and warnings

 **NOTE:** A NOTE indicates important information that helps you make better use of your product.

 **CAUTION:** A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

 **WARNING:** A WARNING indicates a potential for property damage, personal injury, or death.

Copyright © 2017 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

Contents

1 Overview	7
What is installed for Dell Hybrid Cloud System for Microsoft?	7
On-premises software	7
Cloud services—optional	9
Compute cluster	9
Storage cluster	10
Backup infrastructure	10
Virtual machines	10
Network configuration	12
Cloud configuration	12
VMM library configuration	13
About Dell Hybrid Cloud System for Microsoft licensing	14
License requirements for the Dell Hybrid Cloud System for Microsoft infrastructure	14
License activation	14
Active Directory requirements	14
Connecting to DVM	15
Running the script	15
Check Group Policy settings	16
2 Administration	17
What to do first	17
Next steps	17
Verify the product license key	18
Review known issues in this release	20
Ensure that the stamp has the latest approved updates	25
Managing Dell Hybrid Cloud System for Microsoft	25
Accounts to use for management	26
Connecting to management tools	26
How to run runbooks	27
Creating tenant VM networks	27
Configuring VLANs for tenant use	29
Adding tenant VM networks to the cloud	29
Flagging the operating system VHD in the VM templates	29
Enabling guest-specified IP addresses in VMM	30
Creating additional tenant storage shares	30
Using Windows Azure Pack	35
Default Windows Azure Pack configuration	35
Before you go into production	36
Setting up tenant portal access on an isolated network	36
Replacing self-signed certificates	40
Disabling the tenant AuthSite and the admin Windows AuthSite websites	40

Updating to a Security Token Service and re-establishing trust.....	41
How to open the management portal for administrators.....	43
How to open the management portal for tenants.....	43
Offering services to tenants.....	43
Optional configuration.....	49
Automating tasks for efficiency.....	50
Windows Azure Pack API reference content for developers.....	50
Configuring disaster recovery protection.....	50
Step 1: Onboard to Azure Site Recovery.....	51
Step 2: Enable protection on a plan or add-on.....	56
Step 3: Tenants create resources.....	57
Step 4: Configure network mapping.....	57
Step 5: Run a failover.....	58
Step 6: Access replicated VMs.....	61
3 Operations.....	62
Monitoring.....	62
Onboarding to Operational Insights.....	62
Using Operations Manager.....	63
Using Operational Insights.....	65
Backup and recovery.....	65
Onboard to Azure Backup.....	65
Default backup schedule and retention policy.....	69
DPM protection groups.....	70
Disable machine account password rotation on management VMs.....	70
Protecting tenant VMs.....	70
Recovering VMs and databases—high level.....	72
Recovering from management component failures.....	77
Recovering a tenant VM.....	81
Recovering DPM from DPM failures.....	85
Adding extra disks to DPM.....	93
Monitoring DPM.....	95
Using the Dell Hybrid Cloud System for Microsoft data consistency runbooks.....	96
Updating the Dell Hybrid Cloud System for Microsoft.....	100
Overview of the Patch and Update framework.....	100
How to check which update package is installed.....	101
How to obtain update packages.....	101
Shutting down and starting up the stamp.....	101
Before you begin.....	102
Shutting down the stamp.....	102
Starting up the stamp.....	105
Recovering after a power outage.....	109
4 Security.....	114
User accounts and groups that are added by default.....	114
User accounts.....	114

Service accounts.....	115
Groups.....	117
Resetting service account passwords.....	118
Resetting expired service account passwords.....	118
How service accounts are managed.....	124
Important information about the password reset script.....	124
How to run the MCPASSWORDReset script.....	125
Viewing MCPASSWORDReset script logs.....	126
Troubleshooting the MCPASSWORDReset script.....	127
Rotating Windows Azure Pack encryption keys.....	130
Managing antivirus and antimalware.....	130
Overview of default antimalware configuration.....	130
How to run unscheduled antimalware scans.....	131
How to view scan results and respond to malware incidents.....	131
How to update antimalware definitions manually.....	132
How to verify that updates are working.....	132
Managing certificates.....	132
Viewing the certificates.....	133
Replacing self-signed certificates with CA-signed certificates.....	133
Updating certificates about to expire.....	139
Appendix A: Expanding the stamp.....	140
Compute expansion workflow.....	140
Physical installation.....	141
Deploying compute expansion nodes.....	141
Adding another server to backup infrastructure.....	141
Appendix B: Performing a factory reset.....	143
Access and account requirements.....	143
Resetting the backup servers.....	144
Resetting the standalone backup host.....	150
Resetting the storage cluster (<Prefix>-SCL).....	153
Resetting the compute cluster (<Prefix>CCL).....	156
Clean up Active Directory and DNS records.....	159
Clean up artifacts created by Azure Site Recovery.....	159
Delete the VMM server.....	160
Delete the IaaS VMs from failover if needed.....	160
Optionally delete the vault and the associated storage account.....	160
Appendix C: Retrieving cluster names, host names, and IP addresses.....	161
Get cluster names.....	161
Get the cluster IP addresses.....	161
Example 1: Compute clusters.....	161
Example 2: File server clusters.....	161
Example 3: SQL Server clusters.....	162
Get host names and IP addresses for cluster hosts.....	162
Compute cluster host.....	162
File server cluster.....	162

SQL Server cluster.....	162
Get infrastructure VM names and addresses.....	163
Appendix D: Ports and protocols.....	164

Overview

Dell Hybrid Cloud System for Microsoft CPS Standard™, referred to in this guide as Dell Hybrid Cloud System for Microsoft, is an infrastructure-as-a-service (IaaS) solution that allows you to quickly get a hybrid cloud solution up and running in your data center. Built on the Dell hardware, and a foundation of Windows Server 2012 R2 and System Center 2012 R2, Dell Hybrid Cloud System for Microsoft allows you to easily extend your solution to Microsoft Azure. Dell Hybrid Cloud System for Microsoft provides a streamlined experience to onboard to the following services:

- Azure Operational Insights
- Azure Backup
- Azure Site Recovery, for disaster recovery

This Administrators Guide provides an overview of the system, and information about how to administer and operate the Dell Hybrid Cloud System for Microsoft.

IMPORTANT: The recommendations and guidelines in this document are based on industry best practices, CPS Standard architecture requirements, and Dell EMC lab testing. If not followed, the functionality and or management of the solution may not work as designed or expected, and problem resolution may be limited, delayed, or not viable.

Topics:

- [What is installed for Dell Hybrid Cloud System for Microsoft?](#)
- [About Dell Hybrid Cloud System for Microsoft licensing](#)
- [Active Directory requirements](#)
- [Check Group Policy settings](#)

What is installed for Dell Hybrid Cloud System for Microsoft?

The following sections describe the general layout of a Dell Hybrid Cloud System for Microsoft stamp.

These include information about the physical clusters, the virtual machines (VMs) that are installed for management, the storage configuration, and the cloud and library resources.

A “stamp” consists of all compute and storage components that are managed by a single instance of Virtual Machine Manager (VMM).

On-premises software

The Dell Hybrid Cloud System for Microsoft includes the following on-premises software components.

Microsoft-provided software

Table 1. Microsoft software

Product/Software Name	Purpose	TechNet Library Reference
Windows Server 2012 R2 Datacenter Edition	The operating system on all physical hosts and VMs.	Windows Server 2012 R2
System Center Virtual Machine Manager (VMM) 2012 R2	Use to manage the virtualization hosts, networking, and storage resources.	Virtual Machine Manager
System Center Operations Manager (SCOM) 2012 R2	Use to monitor the infrastructure.	Operations Manager
SQL Server 2014	Hosts the databases for infrastructure VMs that require SQL Server.	SQL Server 2014 Product Documentation
Windows Azure Pack	Allows you to offer the IaaS services to your users, through a self-service cloud.	Windows Azure Pack for Windows Server
System Center Data Protection Manager (DPM) 2012 R2	Use to back up both management infrastructure and tenant VMs.	Data Protection Manager
System Center Endpoint Protection	Provides antimalware services to the physical hosts and infrastructure VMs.	Endpoint Protection Client
Service Management Automation (SMA)	Allows you to automate the creation, monitoring, and deployment of resources in your Windows Azure Pack environment.	Service Management Automation
Service Provider Foundation (SPF)	Exposes a web service that interacts with VMM. This allows the Windows Azure Pack portals to interact with the VMM to enable the IaaS capabilities in System Center 2012 R2.	Service Provider Foundation

NOTE: The System Center Data Protection Manager (DPM) runs separately on hosts outside the initial Dell Hybrid Cloud System for Microsoft stamp.

Dell-provided software

Table 2. Software

Product/Software Name	Purpose	More Information
User interface and middle layer	<ul style="list-style-type: none"> Guides deployment workflow Gathers data and generates manifest Adds compute chassis (4 sleds per chassis) 	Provided in the <i>Dell Hybrid Cloud System for Microsoft Cloud Platform System Standard Administrators Guide</i>
Dell Server Management Pack Suite (DSMPS)	Provides hardware health information to the System Center Operations Manager	Dell Server Management Pack Suite

Product/Software Name	Purpose	More Information
Storage Enclosure CLI (SECLI)	<ul style="list-style-type: none"> Updates the Dell PowerVault MD storage enclosure firmware Monitors the modular disk (MD) 	Staged on local disk; see Dell Storage Enclosure Administrator's Guide
BMC Utility	<ul style="list-style-type: none"> Sets firmware Debugs (mostly BMC/iDRAC) 	Staged on local disk; see Dell Storage Enclosure Administrator's Guide
OpenManage Deployment Toolkit	<ul style="list-style-type: none"> Sets firmware Debugs (firmware beyond BMC/iDRAC) 	Staged on local disk; see Dell Open Manage Deployment Toolkit
SupportAssist	Gathers hardware and software information for support group	Staged on local disk; see SupportAssist
OpenManage Server Administrator (OMSA)	OS level hardware health monitoring agent	Staged on local disk; see OpenManage Server Administrator—OMSA
OpenManage Essential (OME)	Support Assist Console	Staged on local disk; see OpenManage Essentials
Repository Manager (RM)	<ul style="list-style-type: none"> Compiles bundle, a collection of server firmware Can use out of band path to update firmware 	Staged on local disk; see Dell OpenManage Repository Manager

Cloud services—optional

You can opt in to these Microsoft services during or after deployment.

During deployment of the Dell Hybrid Cloud System for Microsoft, you are given the option to register for the following Microsoft Azure services:

- Azure Operational Insights, available only in certain regions as seen when you [Onboard to Azure Site Recovery](#).
- Azure Backup
- Operational Insights, also known as Operations Management Suite

Azure Site Recovery is available for opt-in only after deployment.

Instructions for how to opt in to these services are included in this guide.

Compute cluster

All of the physical compute nodes in a Dell Hybrid Cloud System for Microsoft stamp form a single compute cluster. The compute cluster consists of the physical Hyper-V nodes that host the VMs for the management infrastructure and the tenant compute workloads. All of these physical nodes run Windows Server 2012 R2 Datacenter edition (Server Core configuration).

The name of the compute cluster is `<Prefix>CCL`.

NOTE: The `<Prefix>CCL` value that this guide uses for physical computer and VM names is a customer-specified prefix for the Dell Hybrid Cloud System for Microsoft stamp.

Storage cluster

The storage cluster is a two- to four-node Scale-Out File Server (SOFS) that is connected to just a bunch of disks (JBOD) storage. The system uses Storage Spaces with an SOFS to provide shared storage in the form of SMB shares. These SMB shares are used by VMs to store their associated VHD (Virtual Hard Disk) files.

All of these physical nodes run Windows Server 2012 R2 Datacenter edition (Server Core configuration).

- The storage cluster is named `<Prefix>SFS`.
- The Windows name of the storage cluster is `<Prefix>SCL`.

The following table describes the default storage share layout:

Table 3. Default storage share

Share Name	Description	Storage Classification
ManagementShare	Stores the .vhdx files for all the infrastructure VMs on the compute cluster.	ManagementStorage
WitnessShareForCompute	Stores the file share witness for the compute cluster.	ManagementStorage
Share01	The default share for tenant storage.	PrimaryStorage

Backup infrastructure

The backup solution for Dell Hybrid Cloud System for Microsoft consists of one or more Hyper-V hosts with sufficient backup capacity for the stamp. These servers are separate from the Dell Hybrid Cloud System for Microsoft stamp. The servers run Windows Server 2012 R2 Datacenter Edition.

Two VMs that are running Data Protection Manager (DPM) are provisioned on each backup host. The VMs run the full installation of Windows Server 2012 R2 Datacenter edition. The first DPM VM that is provisioned (typically `<Prefix>DPM01`) is the backup server for the management infrastructure VMs. Other DPM server VMs are provisioned to back up tenant workloads.

Virtual machines

The following describes VMs that the Dell Hybrid Cloud System for Microsoft uses.

Infrastructure Virtual Machines

The compute cluster hosts the following infrastructure VMs. These VMs host the resources for Dell Hybrid Cloud System for Microsoft fabric and service management:

- All VMs run Windows Server 2012 R2 Datacenter edition.
- With the exception of the Console VM, all VMs on the compute cluster run Server Core.
- All VMs are highly available. This means that a live migration of the VM occurs if there is a host issue.

Table 4. Infrastructure VMs

VM Name	Role/Component Name
<Prefix>CON01	Console VM
<Prefix>VMM01	VMM Server (Also runs Windows Server Update Services (WSUS) and is the VMM library server.)
<Prefix>APA01	<ul style="list-style-type: none"> Windows Azure Pack management portal for administrators (and other administrator components) Service Provider Foundation (SPF) Service Management Automation (SMA)
<Prefix>APT01	Windows Azure Pack management portal for tenants (and other tenant components)
<Prefix>OM01	Operations Manager
<Prefix>SQL01 <Prefix>SQL02	SQL Server guest cluster

SQL Server guest cluster

The management infrastructure components require SQL Server databases. These databases are partitioned into two instances of SQL Server 2014 which run on a two-node guest failover cluster (the <Prefix>SQL01 and <<Prefix>>SQL02 VMs).

The guest cluster name is <Prefix>SQLCL.

The following table shows the instance of SQL Server names, and the databases on each instance.

Table 5. Guest cluster

Instance Name	Databases
<Prefix>SQLIN01\SQLIN01	Windows Azure Pack databases: <ul style="list-style-type: none"> Microsoft.MgmtSvc.Config Microsoft.MgmtSvc.PortalConfigStore Microsoft.MgmtSvc.Store Microsoft.MgmtSvc.Usage Microsoft.MgmtSvc.WebAppGallery Operations Manager databases: <ul style="list-style-type: none"> OperationsManager (operational database) OperationsManagerDW (data warehouse)
<Prefix>SQLIN02\SQLIN02	<ul style="list-style-type: none"> SCSPFDB (for SPF) SMA (for SMA) SUSDB (for WSUS) VirtualManagerDB (for VMM)

Network configuration

The default Dell Hybrid Cloud System for Microsoft network settings are configured during deployment. By default, there is one logical network that is named `Infrastructure`, with three IP address pools:

- `Management_Pool`
- `Storage1_Pool`
- `Storage2_Pool`

By default, there are three VM networks, **Management**, **Storage1**, and **Storage2**; all are associated with the **Infrastructure** logical network. These have the same associated IP address pools configured as the pools for the logical network.

For more information about networking concepts in VMM, see this [blog post](#).

You must configure VM networks for tenant use, as described in [Create tenant VM networks](#).

Cloud configuration

By default, there is a single cloud for tenant resources. The cloud is named `Tenant Cloud`. This cloud has the following properties in VMM:

NOTE: To view the cloud properties in the VM console, open the VMs and Services workspace. Under Cloud, right-click `Tenant Cloud`, and then click `Properties`.

Table 6. Cloud properties

Resource	Value
Host group	All Hosts
Logical networks	Infrastructure
Load balancers	Microsoft Network Load Balancing (NLB)
Port classifications	All are selected.
Storage classification	PrimaryStorage
Read-only library shares	Name: <code>MSSCVMMLibrary</code> Path: <code>\\<Prefix>VMM01.domain.com\MSSCVMMLibrary</code>
Capacity	All set to <code>Use Maximum</code> .
Custom properties	<code>CreateHighlyAvailableVMRoles: true</code> NOTE: The cloud must have this custom property set to <code>true</code> for the VMs to configure as highly available. <code>SupportedVmGenerationForVmRole: 1</code>

VMM library configuration

The VMM library is a catalog of resources that provides access to file-based resources such as virtual hard disks (VHDs), ISO images, scripts, driver files, and application packages that are stored on library servers. It also provides access to non-file-based resources such as VM templates, service templates, and profiles that reside in the VMM database.

To view the layout of the VMM library, in the VMM console, open the **Library** workspace:

- **Cloud Libraries** -Shows the library share that is available to the cloud that was created for tenant resources.
- **Library Servers** -Shows the VMM library server and the library share. In Dell Hybrid Cloud System for Microsoft, the VMM library server is the same as the VMM server (<Prefix>VMM01). By default, there is one library share.

Table 7. Default library share

Library Share Name	Purpose
MSSCVMMLibrary	<p>The default VMM library share. Also, for tenants, this is the read-only library share that is used to store tenant resources.</p> <p>By default, in the VHDs folder, there are the following virtual hard disk files:</p> <ul style="list-style-type: none">• Core.vhdx• Full.vhdx• Blank Disk – Small.vhdx• Blank Disk – Large.vhdx• Blank Disk – Large.vhd• Blank Disk – Small.vhd

In the library, there are several pre-built VM templates that tenants can use for VM creation. You can view them in the **Library** workspace > **Templates > VM Templates**.

These include:

- **A1** and **A1_Full**
- **A2** and **A2_Full**
- **A3** and **A3_Full**
- **A4** and **A4_Full**

The appended **_Full** indicates that the VM template uses the **Full.vhdx** file for deployment. This deploys the full installation of Windows Server 2012 R2 Datacenter edition. If **_Full** is not indicated, the template uses **Core.vhdx** (the server core configuration). These templates deploy VMs that map to Azure sizing for the number of cores and memory; but not for storage. (To view the properties, right-click a template, click **Properties**, and then click the **Hardware Configuration** tab.)

NOTE: By default, Remote Desktop is not enabled in the operating system image to which these templates point.

For more information about the VMM library, see [Configuring the VMM Library](http://technet.microsoft.com/library/gg610598.aspx) (http://technet.microsoft.com/library/gg610598.aspx) in the Microsoft TechNet Library.

About Dell Hybrid Cloud System for Microsoft licensing

License requirements for the Dell Hybrid Cloud System for Microsoft infrastructure

You need the following licenses for your Dell Hybrid Cloud System for Microsoft installation.

- For Windows Server 2012 R2, and for Microsoft System Center 2012 R2, you need either of the following:
 - A Microsoft volume license for Windows Server 2012 R2 Datacenter edition, and a Microsoft volume license for Microsoft System Center 2012 R2. For more information, see <http://www.microsoft.com/en-us/Licensing/product-licensing/windows-server-2012-r2.aspx> and <http://www.microsoft.com/en-us/Licensing/product-licensing/system-center-2012-r2.aspx>.
 - If you do not have an existing volume license agreement, Dell recommends that you use Core Infrastructure Server Suite Datacenter licenses. This license combines both Windows Server 2012 R2 and System Center 2012 R2. It requires one license per physical node (compute and storage nodes).
- A Microsoft Azure subscription, if you want to opt in to Azure services. Acquire an Azure subscription from Microsoft or an authorized reseller. For more information, see <https://azure.microsoft.com/en-us/pricing/purchase-options/>.

❶ IMPORTANT: The recommendations and guidelines in this document are based on industry best practices, CPS Standard architecture requirements, and Dell EMC lab testing. If not followed, the functionality and or management of the solution may not work as designed or expected, and problem resolution may be limited, delayed, or not viable.

❶ NOTE: Windows Azure Pack does not require a license.

License activation

- The Windows Server license requires activation after deployment. Ensure that the license on each physical host and on each infrastructure VM is activated. For more information, see [Volume Activation Overview](#) in Microsoft TechNet.
 - If you have an existing Key Management Service (KMS) server in the domain or have Active Directory-based activation configured, the licenses should automatically activate.
 - If you do not have either of these mechanisms configured, Dell recommends that you configure Active Directory-based activation as this is the easiest approach.
- The System Center license does not require activation.
- Windows Azure Pack does not require activation.
- Microsoft Azure services do not require activation. However, if it is a new Azure user account, sign in to the [Azure portal](#) and change the password before you opt in to Microsoft Azure services.

Active Directory requirements

Deploy Dell Hybrid Cloud System for Microsoft into an existing Active Directory Domain Services (AD DS) domain. The domain must have:

- At least one domain controller that is running Windows Server 2012 or Windows Server 2012 R2.
- No domain or forest functional level requirements.

When you deploy Dell Hybrid Cloud System for Microsoft, the accounts and objects for the stamp are added to an organizational unit (OU) that is specific to Dell Hybrid Cloud System for Microsoft.

At least 10 hours before deploying Dell Hybrid Cloud System for Microsoft, run the **ADPreCreationTool.ps1** script to:

- Create the parent OU

- Create a Key Distribution Services (KDS) root key that is used to generate group Managed Service Accounts (gMSA)
- Block inheritance.

To run the `ADPreCreationTool.ps1` script, you must have domain administrator credentials.

- ① **NOTE:** Dell strongly recommends that you use the `ADPreCreationTool.ps1` script. If you choose to skip running the script and do not have a KDS enabled, manually create a KDS root key and block inheritance before deployment. Create the KDS root key at least 10 hours before deployment. For more information, see [Create the Key Distribution Services KDS Root Key in Microsoft TechNet](#).
- ① **IMPORTANT:** The recommendations and guidelines in this document are based on industry best practices, CPS Standard architecture requirements, and Dell EMC lab testing. If not followed, the functionality and or management of the solution may not work as designed or expected, and problem resolution may be limited, delayed, or not viable.

You can obtain the script from either of the following locations:

- [Microsoft](#) download, or
- Deployment VM (DVM)

Connecting to DVM

You can connect to a Deployment VM (DVM) on any of the physical hosts in the Dell Hybrid Cloud System for Microsoft stamp. To connect to a DVM:

- 1 Make sure that the stamp is powered on.
- 2 Connect a Windows laptop directly to a 1 Gb port of one of the servers. Make sure that it is the only active connection. IPv6 must be enabled with autoconfiguration. No IPv4 configuration is required.
- 3 Open a Remote Desktop Connection, and connect to DVM by name, using the credentials:
 - `.\Administrator`
 - `<Password provided by Dell Deployment Services>`
- 4 Locate the `ADPreCreationTool` script in the following folder:
`C:\Program Files\Microsoft Cloud Solutions\Tools\`

Running the script

You must run the `ADPreCreationTool` script from a domain-joined computer, logged on as a domain administrator. (You cannot run the script from the DVM.) To run the script:

- 1 Open a Windows PowerShell session.
- 2 Change to the directory in which the script is stored.
- 3 Run the script. The script has only one required parameter — the name of the parent OU to create for Dell Hybrid Cloud System for Microsoft.

For example:

```
PS C:\>.\ADPreCreationTool -OU "<OU_Name>"
```

- ① **NOTE:** `OU_Name` is the name of the parent OU. When you deploy the stamp, a child OU for that particular stamp is created under the parent OU.

When the script runs, it prompts you for a new domain user account credential that is given delegated permissions to the parent OU. (The account is created in the parent OU.) The new domain user account credential is the credential that you use when you deploy Dell Hybrid Cloud System for Microsoft.

Check Group Policy settings

When the deployment process creates the Active Directory organizational unit (OU) for Dell Hybrid Cloud System for Microsoft, it blocks policy inheritance on the OU. If your domain has Group Policy Objects (GPOs) that are configured at a higher OU or domain level with the **No Override** option enabled, these policy settings apply to servers in the Dell Hybrid Cloud System for Microsoft stamp. These policy settings may interfere with the deployment process and cause deployment to fail. In this case, Dell recommends that you disable the **No Override** option during stamp deployment.

IMPORTANT: The recommendations and guidelines in this document are based on industry best practices, CPS Standard architecture requirements, and Dell EMC lab testing. If not followed, the functionality and or management of the solution may not work as designed or expected, and problem resolution may be limited, delayed, or not viable.

Known policy settings that cause deployment to fail include:

- The following policy settings under **GPO_name\Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options**:
 - **Accounts: Administrator account status** (if set to Disabled)
 - **Accounts: Rename administrator account**
- The following policy setting under **GPO_name\Computer Configuration\Policies\Windows Settings\ Security Settings\Account Policies\Password Policy**:
 - **Minimum password length** — if set to >16
- If you have restricted groups configured under **GPO_name\Computer Configuration\Windows Settings\Security Settings \Restricted Groups**.

There are several other policy settings that may block deployment, such as Windows PowerShell settings, disabled services, and Windows Firewall rules that block remote Windows PowerShell.

Administration

This chapter contains detailed information about administrative tasks required for implementing Dell Hybrid Cloud System for Microsoft.

Topics:

- [What to do first](#)
- [Next steps](#)
- [Managing Dell Hybrid Cloud System for Microsoft](#)
- [Creating tenant VM networks](#)
- [Adding tenant VM networks to the cloud](#)
- [Flagging the operating system VHD in the VM templates](#)
- [Enabling guest-specified IP addresses in VMM](#)
- [Creating additional tenant storage shares](#)
- [Using Windows Azure Pack](#)
- [Configuring disaster recovery protection](#)

What to do first

After you deploy the Dell Hybrid Cloud System for Microsoft stamp, you can get up and running by doing the following:

- Adding management accounts
- Familiarizing yourself with the tools
- Checking system health
- Creating tenant VM networks
- Adding tenant VM networks to the cloud
- Flagging the operating system VHD in the VM templates
- Creating additional tenant storage, if you want to do this immediately.

Before you go into production, do the following:

- Replace self-signed certificates
- Disable the default Windows Azure Pack authentication sites
- Update to a Security Token Service such as Active Directory Federation Services (AD FS) and re-establish trust.

NOTE: Optionally, you can set up tenant portal access on an isolated network. See the section [Before you go into production for more information](#).

Next steps

After you complete the deployment of the Dell Hybrid Cloud System for Microsoft stamp, there are additional steps you must complete. These steps include:

- Verify the product license key, as described in the section that follows
- [Enable guest-specified IP addresses in VMM](#)

- [Disable machine account password rotation](#)
- [Deploy the Data Protection Manager \(DPM\) backup infrastructure](#)
- [Ensure that the stamp has the latest approved updates](#)
- [Configure VLANs on your physical network switches for tenant use](#)
- [Review known issues for the current release.](#)

There are other steps, not part of the initial deployment, that you must complete as soon as possible to enable tenants to use the stamp. For example, you must [configure management accounts](#) and [tenant VM networks](#). You may also want to [add storage shares](#).

Verify the product license key

If you specified an incorrect System Center key during deployment, the deployment will complete. However, the Microsoft System Center components will be installed in evaluation mode. After deployment, you should verify that System Center has a valid retail license key.

To verify the license key in VMM:

- 1 On the Console VM, use the shortcut on the desktop to open the VMM console.
- 2 In the top left corner of the VMM console, click the drop-down arrow, and then click **About**.

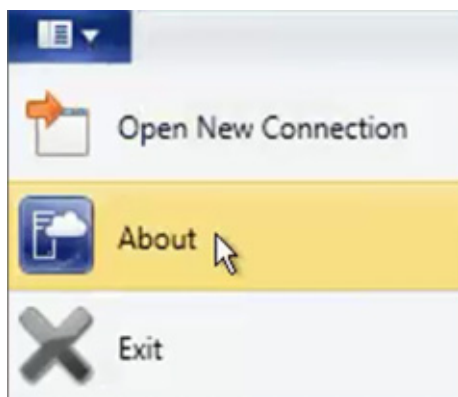


Figure 1. About drop-down

- 3 If you see an **Enter Product Key** box, this means that System Center was installed in evaluation mode.



Figure 2. Enter Product Key box

If you do not see this box, you have a valid retail license key and can skip the rest of this procedure.

What to do if you enter an incorrect product license key

If you specified an incorrect System Center key during deployment, you must update VMM, Operations Manager, and Service Management Automation (SMA) to use a valid System Center product license key.

Run all of the following procedures from an elevated Windows PowerShell session on the Console VM. On the **Start** screen, click the Search icon, and then type `PowerShell`. In the results, right-click **Windows PowerShell**, and then click **Run as administrator**.

To update VMM

Use these procedures to update VMM if you specified an incorrect System Center key during deployment.

- 1 From the elevated Windows PowerShell session, run the following commands, pressing **Enter** after each command:

NOTE: Replace *<Prefix>* with the customer-specific prefix for the Dell Hybrid Cloud System for Microsoft stamp. For *ProductId*, specify the retail System Center license key.

```
Import-Module VirtualMachineManager

$VMMServer = Get-SCVMMServer -ComputerName <Prefix>VMM01

Register-SCVMMAccessLicense -VMMServer $VMMServer -ProductKey "XXXXXX-XXXXXX-XXXXXX-XXXXXX-XXXXXX"
-AcceptEULA
```

- 2 To verify that the license is correct:

```
Get-SCVMMAccessLicense -VMMServer $VMMServer -License
```

The output should indicate a **LicenseType** of **Volume**, as shown in the following example.

```
PS C:\Windows\system32> Get-SCVMMAccessLicense -VMMServer $vmmserver -License

ProductName      : System Center Virtual Machine Manager 2012
LicenseType      : Volume
```

```
LicenseBy      : SML
UnitLabel     : Server
TabulationMethod : Unique
```

```
ProductName    : System Center Virtual Machine Manager 2012
LicenseType   : Volume
LicenseBy     : ManagementServer
UnitLabel     : Server
TabulationMethod : Unique
```

```
ProductName    : System Center Virtual Machine Manager 2012
LicenseType   : Volume
LicenseBy     : VOSE
UnitLabel     : Server
TabulationMethod : Unique
```

To update Operations Manager

Use these procedures to update Operations Manager if you specified an incorrect System Center key during deployment.

- 1 In the elevated Windows PowerShell session, run the following commands, pressing **Enter** after each command:

```
$Credential = Get-Credential
```

```
Enter-PSSession -ComputerName <Prefix>OM01.domain.com -Authentication
CredSSP -Credential $Credential
```

```
Import-Module OperationsManager
```

```
Set-SCOMLicense -ProductId "XXXX-XXXXX-XXXXX-XXXXX-XXXXX"
```

- 2 Press **Y** to confirm.

- 3 Run the following command to restart the System Center Data Access Service.

```
Restart-Service OMSDK
```

- 4 To verify the license update, run the following command:

```
(Get-SCOMManagementGroup).SkuForLicense
```

The output should indicate **Retail**.

- 5 Type `exit` to exit the remote session.

To update SMA

Use these procedures to update SMA if you specified an incorrect System Center key during deployment.

- 1 In the elevated Windows PowerShell session, run the following command:

```
Set-SmaLicense -WebServiceEndpoint "https://<Prefix>APA01" -ProductKey "XXXX-XXXXX-XXXXX-
XXXXX-XXXXX"
```

- 2 To check the license expiration date:

```
(Get-SmaLicense -WebServiceEndpoint "https://<Prefix>APA01").ExpirationDate
```

The expected date is 100 years from now.

Review known issues in this release

The following sections address known issues in this version of Dell Hybrid Cloud System for Microsoft.

Host cluster refresh in VMM results in IP address error

Host cluster refreshes in VMM that are performed on the Dell Hybrid Cloud System for Microsoft compute cluster (named <Prefix>CCL) produce Error 25112, as shown in the following section. Host cluster refreshes are performed automatically after certain operations in Dell Hybrid Cloud System for Microsoft. The error has no immediate effect on operations, but it will continue to occur after each host cluster refresh unless you reassign the IP address to the host cluster. Also, it may cause issues if there is a cluster failover.

Error (25112)

The specified address ((AllocatedIPAddressData#c9c1) { id = 1e0a529c-0d01-4fdc-af7b-64b4aa2f932c, LastUpdatedTimestamp = 8/18/2015 2:31:27 AM }) is already allocated by the pool (**Management_Pool**). This address should be assigned to only a single entity.

Recommended Action

Resolve to which entity this address is allocated.

To resolve this issue, use the [Revoke-SCIPAddress](#) cmdlet in the VMM command shell to revoke the assigned static IP address for the host cluster; then use [Grant-SCIPAddress](#) to reassign the IP address to the host cluster.

You can run the following Windows PowerShell script to find out the IP address (based on the ID provided by the error message), revoke the address, and then reassign the same IP address to the compute cluster. You must run the script on the Console VM; open an elevated session of the VMM command shell.

Substitute the ID from the error message for **\$ID** and the name of the IP address pool. **\$IPPoolName** is **Management_Pool**, the IP address pool for the compute cluster.

⚠ WARNING: The code set off by “Begin - Long Line” and “End - Long Line” is one continuous line of code that has been wrapped to fit in this document. It should be a single line in the script that you save and run.

```
$ID = "0a99a2f5-3516-4ab9-be89-7d9edd3bb0d2"
$IPPoolName = "Management_Pool"

If (-not (Get-Module virtualmachinemanager)) {
Import-Module virtualmachinemanager }

$IP = Get-SCIPAddress | Where-Object {$_.ID -eq $ID}
$IPPool = Get-SCStaticIPAddressPool -Name $IPPoolName

# Look up the DNS Name based on the IP address
$VMHostClusterName = [System.Net.Dns]::GetHostbyAddress($IP.Name)
$VMHostCluster = Get-SCVMHostCluster -Name $VMHostClusterName.HostName

# Release the IP address to the IP pool
Get-SCIPAddress -IPAddress $IP | Revoke-SCIPAddress

# Re-assign the IP address to the host cluster
# Begin - Long Line
Grant-SCIPAddress -GrantToObject Type HostCluster -GrantToObjectID $VMHostCluster.ID -IPAddress
$IP.Name -StaticIPAddressPool $IPPool -Description $VMHostCluster.Name
#End - Long Line
```

VM refresh of the Console VM completes with a warning

After a VM refresh of the Console VM in VMM, you see the following warning. You can ignore this message; the issue has no effect on operations.

Warning (26902)

For a discovered virtual network adapter connected to virtual switch (*Deployment*) on host (KGC17A.1j04.1ab), the VM network cannot be set to (*Management*). This is because the uplink is not configured to include network site (*Management_0*).

Recommended Action

Configure the physical network adapter of the virtual switch to include one or more of the appropriate network sites (logical network definitions), and refresh the host.

Azure Site Recovery entity names differ based on stamp version during onboarding

The naming convention for the Azure Site Recovery entities varies based on the Microsoft update version of the Dell Hybrid Cloud for Microsoft stamp when Azure onboarding was performed. The following table shows the differences. Note that *<Prefix>* is the customer prefix of the Dell Hybrid Cloud for Microsoft stamp.

Table 8. Entity names for ASR

Entity	Azure Onboarding with RTM	Azure Onboarding with U0 Refresh Code	Azure Onboarding with 1603 Code
Resource Group	Not Applicable	<i><Prefix></i> - <i><PartialDeploymentGUID></i>	<i>cps-<PartialDeploymentGUID></i>
Azure Storage Account	<i><Prefix></i> - <i><PartialDeploymentGUID></i>	<i>cps<PartialDeploymentGUID></i>	<i>cps<PartialDeploymentGUID></i>
Vault	<i><Prefix></i> - <i><DeploymentGUID></i>	<i><Prefix></i> - <i><DeploymentGUID></i>	<i>cps-<DeploymentGUID></i>
Protection Policy	Not Applicable	<i><Prefix></i> -ProtectionPolicy	<i>cps-ProtectionPolicy</i>

Cloud mapping job fails during Azure Site Recovery onboarding

During Azure Site Recovery onboarding, the "cloud mapping" job may fail with the following error in the Azure portal:

Error Message: *The operation has failed. (Error Code: 547)*

Possible Causes: *An internal server error occurred. Operation failed because of an internal error.*

Recommended Action: *Wait a while, and retry the action. If the issue persists, contact support.*

In the *<SystemDrive>\ProgramData\Microsoft Cloud Solutions\DeployDriver\Invoke-SiteRecoveryConfiguration.log*, you see errors similar to the following:

*MapCloud Job failed with retryable error. Associating Protection Policy with Tenant Cloud again.
[Cloud Mapping job (ID: '<JobID>') is in 'Failed' state.]*

To work around this issue, after approximately 30 minutes, follow these steps:

- 1 Sign in to the [Azure portal](#).
- 2 Go to **Recovery Services vaults**, and then click the name of the vault for the Dell Hybrid Cloud System for Microsoft deployment. Look for the name *cps-<DeploymentGUID>*.
- 3 In **Settings**, select **Site Recovery Jobs**.
- 4 Restart the **Associate the protection group** job.
- 5 After the job completes successfully, restart Azure Site Recovery onboarding to complete the remaining onboarding steps.

Also, in the `<SystemDrive>\ProgramData\Microsoft Cloud Solutions\DeployDriver\Invoke-SiteRecoveryConfiguration.log`, you may see this error:

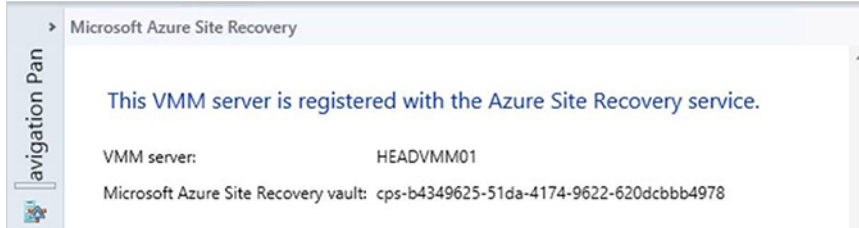
[Cloud 'Tenant Cloud' [ID: 'e4166c98-d1b9-4631-bb83-a8946d7821dd']] is not synced successfully with Azure. Check if SCVMMService is running. Wait for cloud to sync and run Azure Onboarding again.]

You can resolve this issue by doing the following:

- 1 Restart the VMM Service by entering the following commands:

```
Enter-PsSession -ComputerName <Prefix>vmm01
Stop-Service SCVMMService
Start-Service SCVMMService
```

- 2 Go to **VMM Settings > Microsoft Azure Site Recovery**.



- 3 Continue Azure onboarding from the Dell user interface.

Expansion of existing stamp fails with “Decryption failed” error message

Expansion of an existing Dell Hybrid Cloud System for Microsoft stamp fails in the following scenario:

- The Dell Hybrid Cloud System for Microsoft stamp is at Microsoft Update version 1603 or a later version.
- The nodes that you want to add are running an earlier version of the Windows Management Framework (WMF) than what is included in Update 1603.

When these two conditions apply, the expansion deployment fails with the message **“Decryption failed. LCM failed to start desired state configuration manually”** in the verbose logs for the nodes that you want to add.

To avoid this issue, do the following before you run expansion:

- 1 Install WMF 5.0 RTM on the new nodes.

TIP: You can download WMF 5.0 RTM from <https://www.microsoft.com/en-us/download/details.aspx?id=50395>. You need the Win8.1AndW2K12R2-KB3134758-x64.msu package.

- 2 Restart the new nodes.

Paging file not large enough for automatic memory dumps

NOTE: This section does not apply if the Microsoft update version of the Dell Hybrid Cloud System for Microsoft stamp at initial deployment is version 1603 or a later version. To check the update version, see [How to check which update package is installed](#).

The paging file on the physical hosts may not be large enough to support the creation of an automatic memory dump if a server crashes. This file may be required for troubleshooting. Dell recommends that you set the paging file size to 16,384 MB (16 GB).

- 1 On the Console VM, open an elevated Windows PowerShell session, that is, run as Administrator.
- 2 Run the following command, where `<hostname1>`, `<hostname2>`, ... are the names of all physical hosts in the stamp (including any backup hosts):

WARNING: The code set off by “Begin - Long Line” and “End - Long Line” is one continuous line of code that has been wrapped to fit in this document. It should be a single line in the script that you save and run.

```
# Begin - Long Line
Invoke-Command <hostname1>,<hostname2>,... {Set-ItemProperty -Path 'HKLM:\SYSTEM
```

```
\CurrentControlSet\Control\Session Manager\Memory Management' -Name PagingFiles -Value "?:
\pagefile.sys 16384 16384"}
# End - Long Line
```

TIP: To find the host names, you can use the VMM console. Or, to find the host names in a cluster, you can run the following Windows PowerShell command, where *<ClusterName>* is the name of the cluster, such as *<Prefix>CCL* and *<Prefix>SCL*:

```
Get-ClusterNode -Cluster <ClusterName> | Format-Table -Property Name
```

- 3 Restart each host for the setting to take effect. You can do this when it is convenient, such as during a scheduled maintenance window. Note the following:
 - If you are restarting a backup host, first stop any running backup jobs. For more information, see "Step 1: Stop any backups" in [Shutting down the stamp](#).
 - Restart the hosts one at a time. Wait for a host to be up and running before you restart the next.
- 4 You can restart hosts:
 - From the Fabric workspace in the VMM console, by right-clicking a host and then clicking **Restart**, or
 - By using Windows PowerShell.
- 5 To restart hosts from a Windows PowerShell:
 - a Log on to any domain-joined computer (external to the stamp is preferable) with an account that is a member of the *<Prefix>Ops-Admins* group.
 - b Open an elevated Windows PowerShell session.
 - c To restart the remote computer, run the following command, where *HostName* is the name of a physical host:

```
Restart-Computer -ComputerName <HostName> -Force
```
 - d Wait until the host is up and running before you restart the next host.

Reclaim space on the compute cluster nodes

NOTE: This section does not apply if the Microsoft update version of the Dell Hybrid Cloud System for Microsoft stamp at initial deployment is version 1603 or a later version. To check the update version, see [How to check which update package is installed](#).

To reclaim space on the compute cluster nodes, you can manually remove the Console.vhdx file from the local disk on each host:

- 1 On the Console VM, open an elevated Windows PowerShell session, that is, run as Administrator.
- 2 Run the following command, where *<hostname1>*, *<hostname2>*, ... are the names of all physical hosts in the compute cluster.

```
Invoke-Command <hostname1>,<hostname2>,... {Remove-Item D:\VHD\Console.vhdx}
```

TIP: To find the host names, you can use the VMM console or you can run the following Windows PowerShell command, where *<Prefix>* is the stamp prefix.

```
Get-ClusterNode -Cluster <Prefix>CCL | Format-Table -Property Name
```

Onboarding to Operational Insights fails if proxy authentication is required

If your environment requires proxy authentication (using Basic authentication) for internet access, Azure onboarding to Operational Insights (also known as OMS, or Microsoft Operations Management Suite) fails while trying to create the **Run As** account called "AdvisorProxyRunAsAccount" in Operations Manager.

- 1 If you are trying to onboard to Azure during initial stamp deployment, you must temporarily ignore this issue and complete stamp deployment.
- 2 After stamp deployment, do the following:
 - a On the Console VM, open the Operations console.
 - b In the **Administration** workspace, under **Run As Configuration**, right-click **Accounts**, and then click **Create Run As Account**.
 - c Complete the **Create Run As Account Wizard** using the following settings.

Table 9. Wizard settings

Wizard Page	Instructions
General Properties	Run As account type: Select Basic Authentication .
	Display name: Enter the name <code>AdvisorProxyRunAsAccount</code> .
Credentials	Enter the user name and password of the proxy server credentials.
Distribution Security	Accept the default setting.

3 [Onboard](#) to Azure services again.

Onboarding to Operational Insights completes successfully.

A port on the virtual switch has the same MAC as one of the underlying team members

On the Hyper-V compute nodes, including backup hosts, you may see the following warning in the **System** log in the **Event Viewer**:

```
Log Name:          System
Source:            Microsoft-Windows-MsLbfoSysEvtProvider
Date:              <Date>
Event ID:          16945
Task Category:    None
Level:            Warning
Keywords:         Classic
User:             N/A
Computer:         <HostName>
Details:
MAC conflict: A port on the virtual switch has the same MAC as one of the underlying team members on Team Nic Microsoft Network Adapter Multiplexor Driver
```

This event is expected. You can ignore this warning message.

Ensure that the stamp has the latest approved updates

To apply the latest approved software, firmware, and driver updates, follow the instructions provided with the P&U.

NOTE: Do NOT install updates by using any other method than the Dell Hybrid Cloud System for Microsoft patch and update framework. Install only update packages that are tested and approved for the Dell Hybrid Cloud System for Microsoft.

Managing Dell Hybrid Cloud System for Microsoft

Dell Hybrid Cloud System for Microsoft includes a Console VM that you can use for management purposes (<Prefix>CON01). The most commonly-used management tools that are available on the Console VM include the following:

- VMM console
- Operations Manager console
- DPM Administrator console.

There are also tools such as SQL Server Management Studio, Hyper-V Manager, Failover Cluster Manager, and the Windows Server Update Services (WSUS) console.

By default, Remote Desktop is enabled on the Console VM.

To manage Windows Azure Pack, you can connect from a web browser on the Console VM. See [How to open the management portal for administrators](#).

Accounts to use for management

To perform most administrative duties in Dell Hybrid Cloud System for Microsoft, you can add users or groups to the **<Prefix>-Ops-Admins** group in the Active Directory domain that you specified during deployment. (You can find this group in the Organizational Unit (OU) that you specified during deployment.)

Accounts in this group have administrator rights to the following:

- VMM
- Operations Manager
- DPM
- Windows Azure Pack management portal for administrators
- Local administrator access on all infrastructure VMs

To administer SQL Server databases, an account must be a member of the **<Prefix>-Diag-Admins** group. This group is a member of the **sysadmin** role. This group is also a member of the local Administrators group on the physical hosts.

For more information about user accounts and groups in Dell Hybrid Cloud System for Microsoft, see [User accounts and groups that are added by default](#).

Connecting to management tools

The following table includes the tools that you use most often for administration. There are many other tools available on the Console VM. To view all tools, click **Start**, and then click the down arrow. This displays all applications that are installed on the Console VM, for example Windows PowerShell.

Table 10. Management tools

Management Tool	Instructions
Console VM	Use a Remote Desktop Connection to log on to the Console VM. Typically, you would log on as a member of the <Prefix>-Ops-Admins group.
VMM console	<ol style="list-style-type: none">1 On the Console VM, click the Virtual Machine Manager Console icon on the taskbar.2 In the Connect to Server dialog box, the name of the VMM server is prepopulated, for example: <Prefix>VMM01:81003 Click Connect.
Operations Console	On the Console VM, open the Operations Console by using the icon on the taskbar.
Data Protection Manager console	If you deployed the Dell Hybrid Cloud System for Microsoft backup infrastructure, you can connect to the DPM servers, by using either of the following methods: Method 1: Open the DPM Administrator console directly <ol style="list-style-type: none">1 On the Console VM, click the Microsoft System Center Data Protection Manager icon on the taskbar.

Management Tool	Instructions
	<ol style="list-style-type: none"> In the Connect to DPM Server dialog box, specify the DPM server name, for example: <Prefix>DPMA01.contoso.com. Click OK. <p>Method 2: Use the Central Console</p> <ol style="list-style-type: none"> Open the Operations console. In the Monitoring workspace, expand System Center 2012 R2 Data Protection Manager > State Views, and then click DPM servers. Click the DPM server that you want to connect to, and then in the Tasks pane, under DPM Server Tasks, click Manage DPM server.
Windows Azure Pack management portal for administrators	<ol style="list-style-type: none"> On the Console VM, click the Internet Explorer icon on the taskbar. On the Favorites bar, click any of the following: <ul style="list-style-type: none"> Azure Pack Admin Azure Pack Tenant Azure
Windows Azure Pack Management portal for tenants	
Microsoft Azure	
SQL Server Management Studio	On the Console VM, click the SQL Server 2014 Management Studio icon on the taskbar.

NOTE: If you try to open Operations Manager Shell as an administrator, you receive an error. To continue, you must run the following commands each time. Press Enter after each command.

```
cd "$env:SystemDrive\Program Files\Microsoft System Center 2012 R2\Operations Manager\Powershell"

.\OperationsManager\Functions.ps1

.\OperationsManager\Startup.ps1
```

How to run runbooks

Runbooks are Windows PowerShell scripts that provide automation. You can find instructions for running Service Management Automation (SMA) runbooks throughout this guide. You can run them either through the Windows Azure Pack management portal for administrators, or from an elevated Windows PowerShell session on the Console VM.

This guide typically includes instructions for how to run your runbooks through the portal. To do this:

- Log on to the Console VM as a member of the **<Prefix>-Ops-Admins** group, and open Internet Explorer by using the icon on the taskbar.
- On the **Favorites** bar, click **Azure Pack Admin**.
- In the navigation pane, click **Automation**.
- On the **Automation** page, click **Runbooks**.
- To search for a runbook, click the filter (magnifying glass icon), and then type the first part of the runbook name.
- To run the runbook, you can do either of the following:
 - If the runbook you want is already highlighted, click **Start**. If it is not highlighted, click anywhere in the row where the runbook is listed, except for in the **Name** column, to highlight the runbook name. Then, click **Start**.
 - Alternatively, click the runbook **Name**. This opens the runbook details page. To run the runbook from the details page, click **Dashboard**, and then click **Start**.

Creating tenant VM networks

This procedure requires that you have already created VLANs in the physical network for tenant use. During the initial deployment, this may already have been configured on the physical switches as part of your Dell Hybrid Cloud System for Microsoft solution.

You must create VM networks for tenants so they can use and access network resources. All virtual machines must be connected to a VM network. To create tenant VM networks, you must use the **Create-VMMTenantNetwork** runbook. This runbook creates the VLAN-based logical networks and VM networks in VMM for tenant use.

- 1 Use the [How to run runbooks](#) procedure discussed in the preceding section to start the **Create-VMMTenantNetwork** runbook.
- 2 Specify the following parameters:

Input Parameter	Description
DnsServers	<p>A comma-separated list of DNS server IP addresses for the subnet.</p> <p>Optional if Subnet is specified.</p> <p>Example: <i>10.22.0.10,10.24.0.11</i></p>
DnsSuffix	<p>The DNS suffix for the subnet.</p> <p>Optional if Subnet is specified.</p> <p>Example: <i>contoso.com</i></p>
Gateway	<p>The default gateway for the subnet.</p> <p>Optional if Subnet is specified.</p> <p>Example: <i>192.168.0.1</i></p>
LogicalNetworkName	<p>The name of the VMM logical network that will be used for tenant networks.</p> <p>If not specified, the default name of Tenant VLANs will be used.</p>
Name	<p>An optional name that is used to generate the IP address pool name and VM Network name.</p> <p>If not specified, the default name Tenant will be used.</p> <p>The resulting VM Network and IP address pool names would be Tenant – VLAN #, where # is the VLAN ID specified for the network.</p>
PoolEnd	<p>The ending address for the IP address pool.</p> <p>Optional if Subnet is specified.</p> <p>If not specified, the last address in the Subnet will be used.</p> <p>Example: <i>192.168.0.254</i></p>
PoolStart	<p>The starting address for the IP address pool.</p> <p>Optional if Subnet is specified.</p> <p>Example: <i>192.168.0.1</i></p>
Subnet	<p>The IP subnet for the network, in the format IP_Address/Prefix.</p> <p>If not specified, DHCP will be used.</p> <p>Example: <i>192.168.0.0/24</i></p>
UplinkPortProfileName	<p>The exact name of the Uplink Port Profile that was created during deployment.</p> <p>If not specified, the default name <i>UplinkPortProfile</i> is used.</p>

Input Parameter	Description
VlanId	The VLAN ID to assign to the network.

Configuring VLANs for tenant use

For tenants to use and access network resources, you need to create VM networks in VMM. These VM networks must map to VLANs that exist in the physical network. Therefore, you must first configure VLANs on your physical network switches, based on management, application, or tenant requirements for isolation.

Ensure that each added VLAN is available on the trunk for all ports on which the Hyper-V hosts in the Dell Hybrid Cloud System for Microsoft stamp are connected. Note that this does not include the backup server.

Also, configure your routers so that the VLANs are routable to users who will need to connect to VMs on the stamp.

Follow the instructions from the hardware manufacturer of your network switch and router.

Adding tenant VM networks to the cloud

After you create the tenant VM networks, you must add them to the Tenant Cloud in VMM.

- 1 In the VMM console, open the **VMs and Services** workspace.
- 2 Under Clouds, right-click **Tenant Cloud**, and then click **Properties**.
- 3 Click the **Logical Networks** tab.
- 4 Do the following:
 - a Make sure that the **Infrastructure** check box is clear.
 - b Select the check box for each tenant VM network that you want to make available to users when they create their VMs.
- 5 Click **OK**.

Flagging the operating system VHD in the VM templates

For a tenant VM to be protected through Azure Site Recovery, if the tenant uses a VM template to deploy the VM, the operating system virtual hard disk (VHD) must be flagged as such .

This setting is not configured in the default VM templates. Dell recommends that you enable this setting if you ever plan to use Azure Site Recovery. If you do not set it, and later decide to use Azure Site Recovery, you need to set this property manually for each VM that was deployed using the default VM templates.

NOTE: This applies only to VMs that were deployed through a subscription to a plan or add-on that has protection enabled.

To flag the operating system VHD in the VM templates:

- 1 In the VMM console, open the **Library** workspace.
- 2 Under **Templates**, click **VM Templates**.
- 3 For each VM template, do the following:
 - a Right-click the template, and then click **Properties**.
 - b Click the **Hardware Configuration** tab.
 - c Under **Bus Configuration > IDE Devices**, click the virtual hard disk.
 - d Select the **Contains the operating system for the virtual machine** check box, and then click **OK**.

Enabling guest-specified IP addresses in VMM

In VMM, you must enable guest-specified IP addresses for the Medium Bandwidth Adapter port profile. This is required for guest cluster creation because during cluster creation, an IP address must be assigned to the cluster.

To do this, perform the following steps:

- 1 In the VMM console, open the **Fabric** workspace.
- 2 Expand **Networking**, and then click **Port Profiles**.
- 3 Double-click **Medium Bandwidth Adapter**, and then click **Security Settings**. The following dialog box opens.

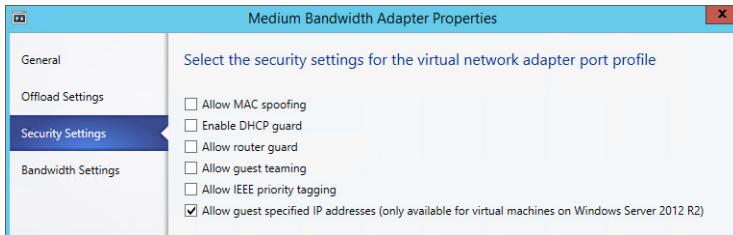


Figure 3. Medium Bandwidth Adapter Properties

- 4 Select the **Allow guest specified IP address (only available for virtual machines on Windows Server 2012 R2)** check box.

Creating additional tenant storage shares

By default, there is only one tenant storage share—Share01. This share is approximately 220 GB, and is used for any Patch and Update packages that are applied to the solution.

You can deploy additional tenant shares as needed, depending on anticipated usage and types of workloads. To create an additional tenant share:

- 1 Create a script similar to the following sample and save it to `\\<prefix>S6\C$\Dell\Scripts`. The values for `$VolumeFriendlyName`, `$SSDSIZE`, and `$HDDSIZE` listed under “# Input Parameters” may need to be changed to reflect the needs of your environment. Dell recommends that the total share size (inclusive of both SSD and HDD) be 10 TB or less.

⚠ WARNING: Each of the following segments of code set off by “Begin - Long Line” and “End - Long Line” are continuous lines of code that have been wrapped to fit in this document. Each should be a single line in the script that you save and run. Also, note that the phrase “Physical Disk” contains a space between these two words.

Table 11. Sample script for creating tenant share

```
# Create a Tenant Share

# Input Parameters
$VolumeFriendlyName = "TenantShare"
$SSDSIZE = [uint64]50GB
$HDDSIZE = [uint64]500GB

# Static Code
$ssdTier = Get-StorageTier -FriendlyName "SSDTier-StoragePool"
$hddTier = Get-StorageTier -FriendlyName "HDDTier-StoragePool"
```

```

# Begin - Long Line 01

New-Volume -StoragePoolFriendlyName "StoragePool" -FriendlyName $VolumeFriendlyName -ResiliencySettingName "Mirror" -
ProvisioningType "Fixed" -StorageTiers $ssdTier,$hddTier -StorageTierSizes $SSDSIZE,$HDDSIZE -FileSystem NTFS -
PhysicalDiskRedundancy 1 -NumberOfColumns 2 -NumberOfDataCopies 2

# End - Long Line 01

#Begin - Long Line 02

$ClusterDiskName = (Get-ClusterResource | Where-Object {($_.ResourceType -match "Physical Disk")}) | Get-ClusterParameter
VirtualDiskName | Where-Object {($_.Value -match $VolumeFriendlyName)}.ClusterObject.Name

#End - Long Line 02

if ($ClusterDiskName)
{
Write-Verbose -Message "$functionName Virtual disk name: $VolumeFriendlyName, Add the disk to CSV."

$csVolume = Add-ClusterSharedVolume -Name $ClusterDiskName
}

$dir = $csVolume.SharedVolumeInfo.FriendlyVolumeName

md $dir\Shares\$VolumeFriendlyName

New-SmbShare -Name $VolumeFriendlyName -Path $dir\Shares\$VolumeFriendlyName -ContinuouslyAvailable $true

```

The following table describes three important parameters to consider when you are creating a new share:

Table 12. Parameters

Parameter	Default Setting	Description
PhysicalDiskRedundancy	1	Number of failed disks that the new share can handle.
NumberOfColumns	2	Number of underlying physical disks across which one stripe of data for a virtual disk is written.
NumberOfDataCopies	2	<p>Settings you can use to configure mirroring:</p> <ul style="list-style-type: none"> 2, the default setting, creates a two-way mirror. 3 creates a three-way mirror, or specifies dual parity. <p>NOTE: 2x2 configurations provide 2-way mirroring, and 2x3 configurations provide 2-way mirroring plus enclosure awareness. To support 3-way mirroring, you must have a 2x4 configuration, which provides 3-way mirroring plus enclosure awareness.</p> <p>IMPORTANT: If you are using exclusively SSDs, you are limited to a 2x2 configuration.</p>

- From the Console VM, start a PowerShell with elevated rights. Type `Enter-PSsession` followed by the name of the Storage node where the script was saved, browse to where the script is located, and run it.
- Connect to the Virtual Machine Manager (VMM) console.



Figure 4. Connecting to VMM

- 4 Browse to **Fabric > Storage > Providers > {Prefix}SCL**.

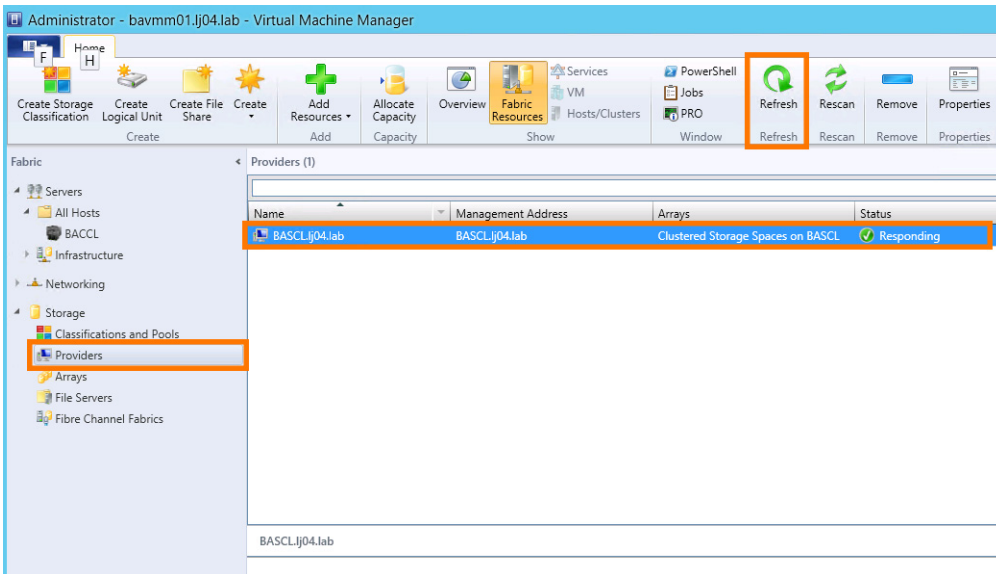


Figure 5. Provider information

- 5 Press **Refresh**.
- 6 Select **File Servers** and right-click on the new share to bring up **Properties**.

NOTE: It may take a few seconds for the recently created file share to appear.

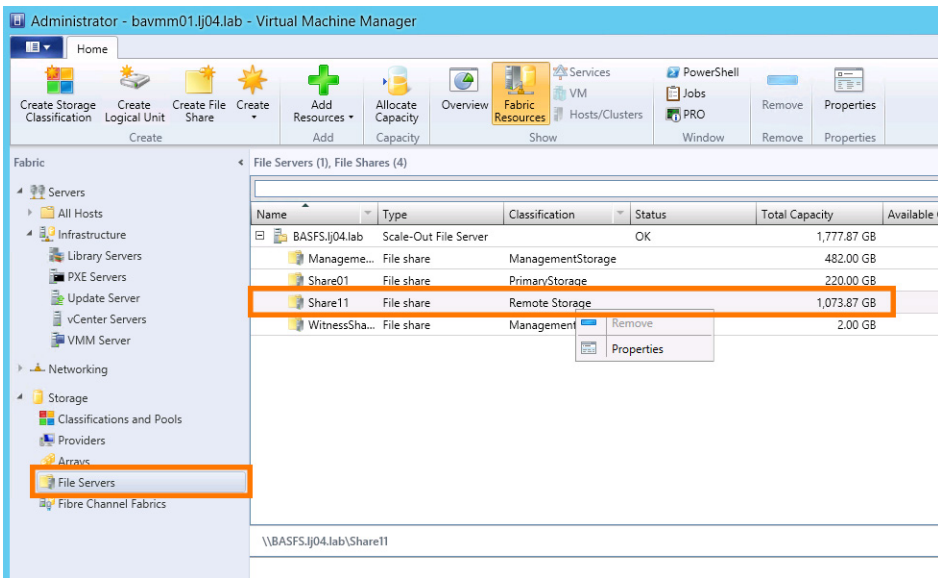


Figure 6. File Server shares

- 7 Check the box to let VMM manage the file share and set **Classification** to **Primary Storage**.

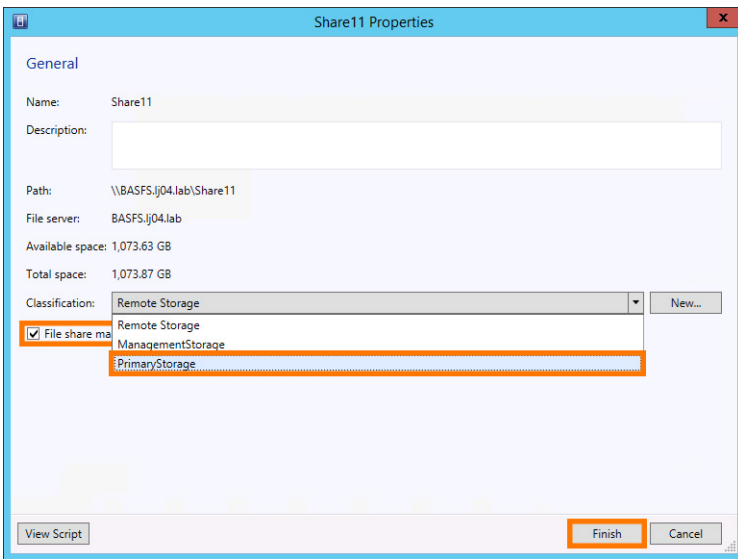


Figure 7. Share properties

- 8 Register the share to the compute cluster. Expand the **Servers**, and right-click on the **Compute Cluster** to bring up its properties.

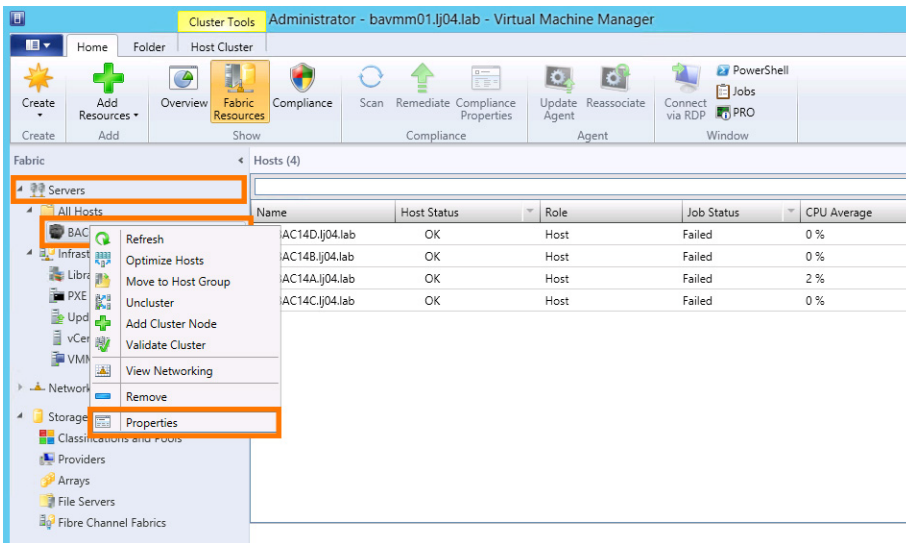


Figure 8. Registering the share

9 Then select **File Share Storage**, click **Add**, and select the new share.

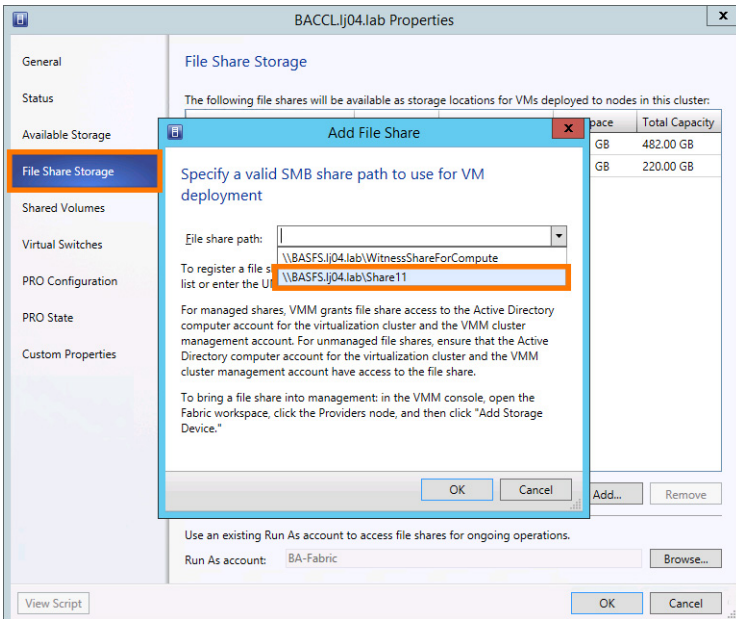


Figure 9. Adding the file share

10 The new **File Share** is made available for VM deployment on the Compute Cluster within a few minutes.

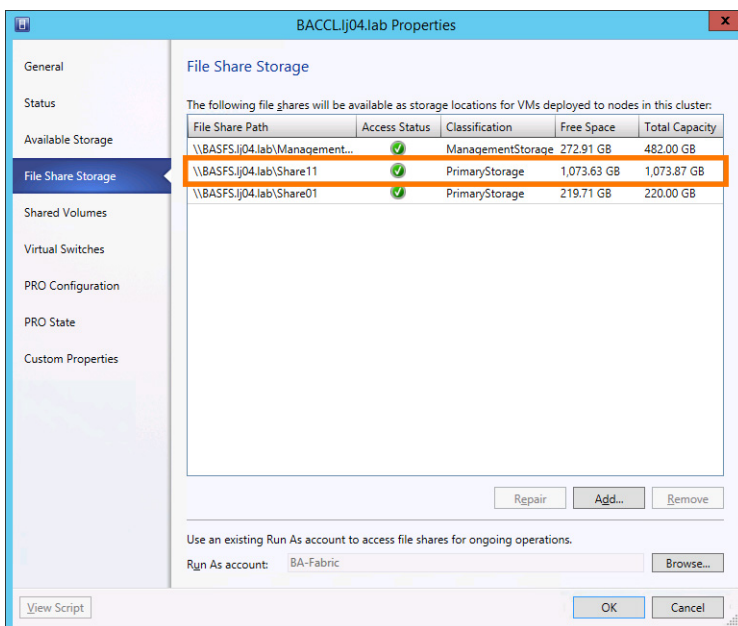


Figure 10. New file share storage available

Using Windows Azure Pack

With Windows Azure Pack, you can offer rich, self-service cloud IaaS services.

With the Dell Hybrid Cloud System for Microsoft solution, you can easily provision and offer virtual machines and VM roles for your users. All components needed for IaaS through the Virtual Machine Cloud resource provider are already installed, with the required integration already configured.

To read about how to manage Windows Azure Pack, see [Administer Windows Azure Pack for Windows Server](#) on Microsoft TechNet.

Default Windows Azure Pack configuration

In the Dell Hybrid Cloud System for Microsoft, the Windows Azure Pack components are installed on two VMs, as described in the following table.

Table 13. Windows Azure Pack VMs

VM Name	Purpose
<Prefix>APA01	<p>Hosts the Windows Azure Pack admin components. These include:</p> <ul style="list-style-type: none"> • Management portal for administrators— A portal for administrators to configure and manage resource clouds, user accounts, tenant plans, quotas, and pricing. In this portal, administrators create plans, and manage user subscriptions. • Admin API— Exposes functionality to complete administrative tasks from the management portal for administrators or through the use of Windows PowerShell cmdlets. • Tenant API— Enables tenants to manage and configure cloud services that are included in the plans that they subscribe to. • Admin authentication site— By default, Windows Azure Pack uses Windows authentication for the administration portal. Before going into production, you must disable this site and use AD FS or an external third-party identity system that supports Web Services Federation (WS-Federation) and JWT tokens to authenticate users.

VM Name

Purpose

<Prefix>APT01

 | **NOTE: This VM also runs SMA and SPF.**

Hosts the Windows Azure Pack tenant components. These include:

- **Management portal for tenants**— A customizable self-service portal to provision, monitor, and manage services. In this portal, users sign up for services and create services, VMs, and databases.
- **Tenant Public API**— Enables tenants to manage and configure cloud services that are included in the plans that they subscribe to. Can be exposed to the internet to provide command line access.
- **Tenant authentication site**— By default, Windows Azure Pack uses an ASP.NET Membership provider to provide authentication for the management portal for tenants. Before going into production, you must disable the ASP.NET provider, and use AD FS or an external third-party identity system that supports WS-Federation and JWT tokens to authenticate users.


For more information, see [Windows Azure Pack components](http://technet.microsoft.com/library/dn469332.aspx) (<http://technet.microsoft.com/library/dn469332.aspx>) in the Microsoft TechNet Library.

Before you go into production

Dell Hybrid Cloud System for Microsoft installation prepares Windows Azure Pack for you to use, but there are some important things you must do before you go into production.

You must:

- Replace self-signed certificates for the Windows Azure Pack websites, SMA, and SPF with trusted SSL certificates that are issued by a trusted certification authority (CA).
- Disable both the default tenant and admin authentication websites.
- Update both tenant and admin authentication to use a security token service such as AD FS or an external third-party identity system.

 **NOTE: There is also an optional procedure to set up tenant portal access on an isolated network. If you want to do this, you must set up the tenant portal access before you replace self-signed certificates and configure integration for AD FS or some other security token service.**

Procedures for all these steps are included in the following sections.

Setting up tenant portal access on an isolated network

The following is an optional procedure you can do before you go into production.

When the Dell Hybrid Cloud System for Microsoft is deployed, all management VMs are connected to the Management network. This includes the VM that hosts the Windows Azure Pack management portal for tenants, <Prefix>APT01, the portal that tenants use to access cloud services.

Sometimes, you may want to isolate the management network from tenant access. Follow the steps in this section if your organization requires network level isolation between the tenant portal and other management VMs. This requirement is more common for cloud service providers.

To isolate traffic, the Windows Azure Pack management portal for tenants VM, referred to as the tenant portal VM, must be connected to another network that is accessible by tenants. This section describes the general requirements and the steps to configure tenant access to the portal over the isolated network.

NOTE: Dell recommends that you set up tenant access isolation before you replace self-signed certificates and configure AD FS, or another security token service. In the process of setting up tenant portal access on an isolated network, you change the fully qualified domain name (FQDN) of the tenant portal in the tenant portal settings. It is best to make the change first, before you undertake the other procedures.

Sample naming convention

IMPORTANT: Your domain name should be the same as the DNS zone in which your DHCS stamp resides. For example, if your domain name is *mycompany.local*, and you are using a DNS zone other than *mycompany.local*, you have a disjointed namespace. The use of disjointed namespaces has not been tested in the DHCS stamp. Dell recommends that you do not use a disjointed namespace within the DHCS stamp.

Examples in this section use the following sample names and addresses:

- Management network: **VLAN 100**
- Tenant access network: **VLAN 110**
- Management network address: **10.10.55.0/26**
- Internal network range: **10.0.0.0/8**
- Dell Hybrid Cloud System for Microsoft stamp prefix: **DHCS**
- Internal domain name—in which the DHCS stamp is deployed: **contoso.local**
- External domain name: **contoso.com**
- Tenant portal VM internal IP address: **10.10.55.14**
- Tenant portal VM internal FQDN: **dhcsapt01.contoso.local**
- Tenant portal VM external IP address: **172.31.1.5**
- Tenant portal VM external FQDN: **cloudportal.contoso.com**

Network requirements

The following diagram illustrates the network configuration for isolated tenant portal access, with examples:

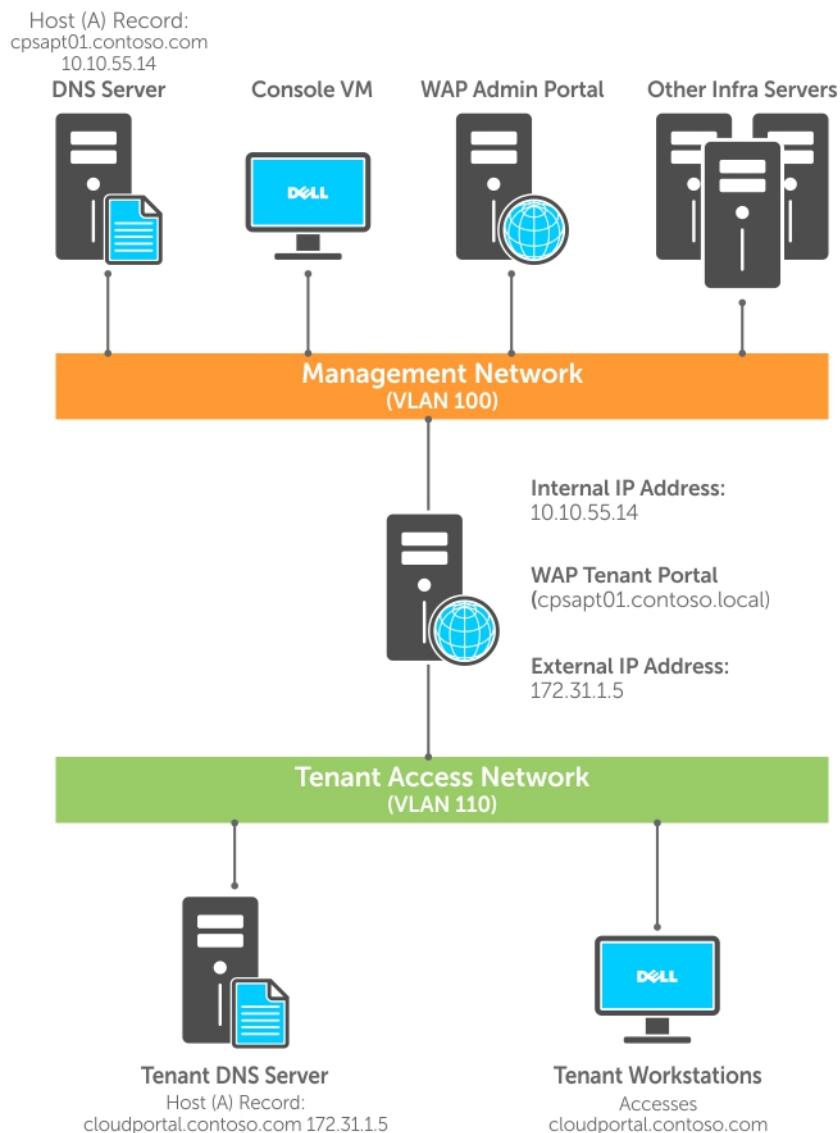


Figure 11. Isolated tenant portal network configuration

Here are the network requirements for this configuration:

- 1 **Tenant access network as a separate VLAN.** You must create a tenant access network as a separate VLAN, for example, VLAN 110, tagged to all ports of the network switches where DHCS servers are connected.
- 2 **A DNS server that tenants use for name resolution.** Typically, this is a different DNS server from the DNS that supports the Active Directory Domain Services (AD DS) infrastructure for DHCS servers, for example, contoso.com. Ensure that the tenant DNS server can resolve internet addresses. This is needed for certificate revocation checks when accessing the tenant portal over SSL. If tenants cannot resolve internet addresses, the tenant portal may take up to 30 seconds to load.
- 3 **An external FQDN for the tenant portal VM.** This fully qualified domain name (FQDN) is the name that tenants use to access the tenant portal, for example, *cloudportal.contoso.com*. Create a Host (A) record on the tenant DNS server that points to the external IP address of the tenant portal VM. (For the external IP address, pick an IP address from the IP subnet that you want to use for the tenant access VLAN.)
The external FQDN of the tenant portal VM must be resolvable by clients on the tenant access network and the management network. Therefore, you must configure a DNS zone with a DNS entry for the external FQDN and IP address of the tenant portal VM on both management and tenant DNS servers.

- 4 **The local routing table of the tenant portal VM must have required routes.** There is no requirement for the tenant access network to route to the management network. However, you must configure the local routing table of the tenant portal VM to correctly route traffic to both the tenant access network and the management network, and to domain controllers for the internal domain (for example, *contoso.local*) that may be on different networks routable to the management network. The step-by-step instructions in the next section show how to configure this.

Configuring the tenant portal

Follow these steps to configure the tenant portal for tenant access through an isolated network:

- 1 Make sure that DNS is configured as described in [Network requirements](#). In particular, make sure a static Host (A) record was created on the DNS servers in both the management and the tenant access networks.
- 2 Configure the physical network devices with a separate VLAN-based network to use for the tenant access network.
- 3 Follow the steps in [Create tenant VM networks](#) to create a tenant access network. This should be a unique network from VM networks that you create for tenant VM use. When you configure runbook parameters, specify the external (tenant-facing) DNS server and DNS suffix.
- 4 In the VM console, do the following:
 - a Open the **VMs and Services** workspace. Click **VM Networks**, and verify that the tenant network was created successfully.
 - b In the navigation tree, click **All Hosts**. In the **VMs** pane, right-click the tenant portal VM **<Prefix>APT01**, and then click **Shut Down**. Click **Yes** to confirm.
 - c After the VM shuts down, right-click the VM, and then click **Properties**.
 - d Click the **Hardware Configuration** tab, click **New** on the toolbar (the green plus sign), and then click **Network adapter**.
 - e In the **Connectivity** area of the new network adapter details, click **Connected to a VM network**. Click **Browse**, select the tenant network you created earlier, and then click **OK**.
 - f Wait until the VM configuration updates. Then, right-click the VM, and click **Power On**.
 - g After the VM starts, right-click the VM, point to **Connect** or **View**, and then click **Connect via Console**. Log in with a user account that has administrative rights.
- 5 On the tenant portal VM, open an elevated Windows PowerShell session and configure IP properties of the new connection. The following example commands disable dynamic DNS registration on the new connection, configure a new IP address on the new interface, and configure a static local routing table as described earlier in [Network requirements](#). The example assumes that there are no DHCP servers on either of the networks. Replace the values in this example with values specific to your network.
 - a Assigns the variable \$if1 to the network interface on which the default gateway is configured (in this case, the interface on the management network).


```
$if1 = Get-NetRoute DestinationPrefix 0.0.0.0/0 | Select-Object -ExpandProperty InterfaceIndex
```
 - b Assigns the variable \$if2 to the interface that is being used for the tenant access network.


```
$if2 = Get-NetIPAddress -AddressFamily IPv4 SuffixOrigin Link | Select-Object -ExpandProperty InterfaceIndex
```
 - c Disables dynamic DNS registration on the new connection.


```
Set-DnsClient -InterfaceIndex $if2 -RegisterThisConnectionsAddress $false
```
 - d Configures a new IP address on the new interface.


```
New-NetIPAddress InterfaceIndex $if2 IPAddress 172.31.1.5 PrefixLength 24
```
 - e Configures a static route to the management network's gateway address.


```
New-NetRoute DestinationPrefix 10.0.0.0/8 NextHop 10.10.55.1 InterfaceIndex $if1
```
 - f Removes the existing default gateway.


```
Remove-NetRoute DestinationPrefix 0.0.0.0/0 Confirm:$false
```
 - g Configures a default route 0.0.0.0/0 to the default gateway of the tenant access network.


```
New-NetRoute DestinationPrefix 0.0.0.0/0 NextHop 172.31.1.1 InterfaceIndex $if2
```
- 6 On the tenant portal VM, in an elevated Windows PowerShell session, run the following commands to configure tenant portal settings. Replace the values in this example with values specific to your network.


```
$sql = 'DHCSSQLIN01\SQLIN01'
```

```
$fqdn = 'cloudportal.contoso.com'
```

```

$pdb = 'Microsoft.MgmtSvc.PortalConfigStore'
$mdb = 'Microsoft.MgmtSvc.Store'
$pcs = "Data Source=$sql; Initial Catalog=$pdb; Integrated Security=True"
$mcs = "Data Source=$sql; Initial Catalog=$mdb; Integrated Security=True"
$mdeip = "https://$fqdn`:30081/FederationMetadata/2007-06/FederationMetadata.xml"
$mderp = "https://$fqdn`:30071/FederationMetadata/2007-06/FederationMetadata.xml"

Set-MgmtSvcFqdn -NameSpace TenantSite -FullyQualifiedDomainName $fqdn
-Port 30081 -PortalConnectionString $pcs -ManagementConnectionString
$mcs

Set-MgmtSvcFqdn -NameSpace AuthSite -FullyQualifiedDomainName $fqdn
-Port 30071 -PortalConnectionString $pcs -ManagementConnectionString
$mcs

Set-MgmtSvcFqdn -NameSpace TenantPublicAPI -FullyQualifiedDomainName
$fqdn -Port 30006 -PortalConnectionString $pcs -ManagementConnectionString
$mcs

Set-MgmtSvcIdentityProviderSettings -Target Membership -MetadataEndpoint
$mdeip -PortalConnectionString $pcs -ManagementConnectionString $mcs
-DisableCertificateValidation

Set-MgmtSvcRelyingPartySettings -Target Tenant -MetadataEndpoint $mderp
-PortalConnectionString $pcs -ManagementConnectionString $mcs -DisableCertificateValidation

```

7 Validate that you can access the Windows Azure Pack management portal for tenants from the tenant access network.

Replacing self-signed certificates

The self-signed certificates that are generated as part of Dell Hybrid Cloud System for Microsoft installation are intended to be temporary. As a security best practice, before you begin using Windows Azure Pack in production, you should promptly replace self-signed certificates with Secure Sockets Layer (SSL) certificates that are issued by a trusted certification authority (CA), such as VeriSign or Thawte. For detailed information about how to do this, see [Replacing self-signed certificates with CA-signed certificates](#).

Disabling the tenant AuthSite and the admin Windows AuthSite websites

NOTE: Before you do this, make sure you have replaced the self-signed certificates.

By default, Dell Hybrid Cloud System for Microsoft uses the following authentication methods for the Windows Azure Pack portals:

- An ASP.NET membership provider database for tenant authentication
- Windows Authentication for the management portal for administrators.

Both of these authentication methods are not supported in a Dell Hybrid Cloud System for Microsoft production environment. Before you go into production, you must shut down the default tenant authentication site (the `AuthSite`) and the default admin authentication site (`WindowsAuthSite`), and then update to a security token service to make authentication more secure.

WARNING: If you shut down the default tenant and admin authentication sites, but do not update to a security token service, nobody can access the management or tenant portals.

When you disable either site, you have the following two options:

- You can stop the website and close the firewall port. This option enables you to easily re-enable the site at any time if needed for troubleshooting.
- You can completely remove the site components from the VM. This includes the Windows Installer Package (.msi file) and the entries from the Operations Manager management pack. This option helps to increase security by reducing the attack surface.

Disabling the tenant AuthSite website

- 1 On the Console VM, open a Windows PowerShell session as an administrator, and then run the following command: **Enter-PSSession -ComputerName <Prefix>APT01**
 - 2 Do either of the following:
 - To stop the authentication site, but not remove the components, run the following command: **Get-Website | Where-Object {\$_.Name -eq "MgmtSvc-AuthSite"} | Stop-Website -Verbose**
 - To completely remove the site components, run the following command: **\$productCode = (Get-ItemProperty -Path HKLM:\SOFTWARE\Microsoft\MgmtSvc\AuthSite).ProductCode**
if (\$productCode){msiexec /x \$productCode -qn}
 - 3 Run the following command to close the Windows Firewall port for the site. By default, this is port 30071. To determine the port, type **Get-Website**. The port is listed under **Bindings**. **Disable-NetFirewallRule -DisplayName "MgmtSvc-AuthSite (HTTPS-In)"**
- NOTE:** This step fails if you have completely removed all components using the second option in the previous step.
- 4 Type **exit** to exit the remote session.

Disabling the admin WindowsAuthSite website

- 1 Open a Windows PowerShell session as an administrator, and then run the following command: **Enter-PSSession -ComputerName< Prefix>APA01**
 - 2 Do either of the following:
 - To stop the authentication site, but not remove the components, run the following command: **Get-Website | Where-Object {\$_.Name -eq "MgmtSvc-WindowsAuthSite"} | Stop-Website -Verbose**
 - To completely remove the site components, run the following command: **\$productCode = (Get-ItemProperty -Path HKLM:\SOFTWARE\Microsoft\MgmtSvc\WindowsAuthSite).ProductCode**
if (\$productCode){msiexec /x \$productCode -qn}
 - 3 Run the following command to close the Windows Firewall port for the site. By default, this is port 30072. To determine the port, type **Get-Website**. The port is listed under **Bindings**. **Disable-NetFirewallRule -DisplayName "MgmtSvc-WindowsAuthSite (HTTPS-In)"**
- NOTE:** This step fails if you have removed all components using the second option in the previous step.
- 4 Type **exit** to exit the remote session.

Updating to a Security Token Service and re-establishing trust

You must update both tenant and admin authentication to use a security token service such as AD FS or an external third-party identity system that supports WS-Federation and JWT tokens.

To set up trust with an external third-party identity system that supports WS-Federation and JWT tokens, you can use the federation metadata file exposed by the Identity Provider.

The following procedures show how to update both tenant and admin authentication to use AD FS as the identity system.

- 1 **Set up trust between the AD FS instance and the Windows Azure Pack management portal for administrators.**
For information about how to set up an AD FS instance through the user interface, and how to set up trust between the AD FS instance and the Windows Azure Pack management portal for administrators, see the following blog posts:

- [Federated Identities to Windows Azure Pack through AD FS – Part 1 of 3](#)
- [Federated Identities to Windows Azure Pack through AD FS – Part 2 of 3](#)

For additional information, see [Configure Active Directory Federation Services for Windows Azure Pack](#) and [AD FS 2.0 Cmdlets in Windows PowerShell](#) in the TechNet Library.

2 Configure the tenant authentication site to trust AD FS.

Connect to the tenant portal VM (**<Prefix>-APT01**), open a Windows PowerShell session, and run the following script.

NOTE: First, replace the values in bold.

For username and password values, specify the username and password of a user who is a member of the **<Prefix>-Diag-Admins** group.

```
$fqdn = "<adfs.contoso.com"
$dbServer = "<Prefix>SQLIN01\SQLIN01"
$dbUser = "username"
$dbPassword = "password"
$portalConfigStoreConnectionString = [string]::Format('Data Source={0};Initial
Catalog=Microsoft.MgmtSvc.PortalConfigStore;User ID={1};Password={2}', $dbServer, $dbUser,
$dbPassword)
Set-MgmtSvcRelyingPartySettings -Target Tenant `
    -MetadataEndpoint https://$fqdn/FederationMetadata/2007-06/FederationMetadata.xml `
    -ConnectionString $portalConfigStoreConnectionString `
    -DisableCertificateValidation
```

3 Configure AD FS to trust the tenant portal.

As an AD FS administrator, run the following Windows PowerShell script on the server on which AD FS is installed. Replace the values in bold. For more information, see [Configure Active Directory Federation Services for Windows Azure Pack](#).

```
$tenantRelyingPartyName = "Management Service - Tenant Site - 2012"
$tenantPortalUrl = "https://myfqdn:port"
$tenantRelyingPartyMetadataEndpoint = "$tenantPortalUrl/FederationMetadata/2007-06/
FederationMetadata.xml"
$identityProviderName = "Identity Provider Name - ex:Active Directory"

$transformationRules = (
    "@RuleTemplate = "LdapClaims" @RuleName = "UPN - LDAP" c:[Type == "http://
schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
AUTHORITY"] => issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/ws/
2005/05/identity/claims/upn"), query = ";userPrincipalName;{0}", param = c.Value);",
    "@RuleTemplate = "LdapClaims" @RuleName = "Groups - LDAP" c:[Type == "http://
schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD
AUTHORITY"] => issue(store = "Active Directory", types = ("http://schemas.xmlsoap.org/
claims/Group"), query = ";tokenGroups(domainQualifiedName);{0}", param = c.Value);",
    "@RuleTemplate = "PassThroughClaims" @RuleName = "UPN - Passthrough" c:[Type ==
"http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"] => issue(claim = c);",
    "@RuleTemplate = "PassThroughClaims" @RuleName = "Groups - Passthrough" c:[Type
== "http://schemas.xmlsoap.org/claims/Group"] => issue(claim = c);")

$issuanceRules = (
    "> issue(Type = "http://schemas.microsoft.com/authorization/claims/permit", Value
= "true");")

$impersonationRules = (
    "c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid",
Issuer =~"^(AD AUTHORITY|SELF AUTHORITY|LOCAL AUTHORITY)$" ] =>
issue(store=" ProxyCredentialStore", types=("http://schemas.microsoft.com/authorization/
claims/permit"),query="isProxySid({0})", param=c.Value );c:[Type == "http://
schemas.microsoft.com/ws/2008/06/identity/claims/groupsid", Issuer =~"^(AD AUTHORITY|SELF
AUTHORITY|LOCAL AUTHORITY)$" ] => issue(store=" ProxyCredentialStore",types=("http://
schemas.microsoft.com/authorization/claims/permit"),query="isProxySid({0})",
param=c.Value );c:[Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/
```

```

proxytrustid"", Issuer =~ ""^SELF AUTHORITY$" ] =>
issue(store="" ProxyCredentialStore", types=(""http://schemas.microsoft.com/authorization/claims/permit""), query=""isProxyTrustProvisioned({0})"", param=c.Value );")

Add-AdfsRelyingPartyTrust `
-Enabled $true `
-Name "$tenantRelyingPartyName" `
-MetadataUrl "$tenantRelyingPartyMetadataEndpoint" `
-EnableJWT $true `
-AllowedClientTypes None `
-ClaimsProviderName @($identityProviderName) `
-IssuanceTransformRules ([System.String]::Concat($transformationRules)) `
-IssuanceAuthorizationRules ([System.String]::Concat($issuanceRules)) `
-ImpersonationAuthorizationRules ([System.String]::Concat($impersonationRules))

```

How to open the management portal for administrators

You can manage and provide Windows Azure Pack IaaS services through the Windows Azure Pack management portal for administrators. Using the Windows Azure Pack management portal for administrators, you can create plans, each of which provides some combination of services that you offer. Tenants then subscribe to the plans that meet their needs.

If you open Internet Explorer on the Console VM, this site is already listed as **Azure Pack Admin** on the **Favorites** bar. The actual site is **https://<Prefix>APA01.domain:30091**.

When you try to access the site, if you have not yet replaced the self-signed certificates, you will see a page saying "**There is a problem with this website's security certificate.**" To bypass this, click **Continue to this website (not recommended)**. You may have to click this two times.

The first time you open the site, click the **X** to close the **New** options.

How to open the management portal for tenants

Tenants can subscribe to plans and provision stand-alone VMs and VM roles through the Windows Azure Pack management portal for tenants.

Stand-alone VMs are single unit virtual machines. VM roles are scalable service tiers consisting of one or more virtual machine instances.

If you open Internet Explorer on the Console VM, the tenant site is already listed as **Azure Pack Tenant** on the **Favorites** bar. The actual site is **https://<Prefix>ATP01.domain:30081**.

When you try to access the site, if you have not yet replaced the self-signed certificates, you see a page saying "**There is a problem with this website's security certificate.**" To bypass this, click **Continue to this website (not recommended)**. You may have to click this two times.

Offering services to tenants

You can use the management portal for administrators to create various plans to which Tenants can subscribe.

Dell Hybrid Cloud System for Microsoft already includes a sample plan, named **TenantPlan**, that you can use to deploy a VM. The plan is public. This means that users can view the plan in the tenant portal and subscribe to the plan. You can find a walkthrough of how to use this plan in the following section.

As an administrator, you must do the following to offer services to tenants:

- 1 Create resources that you want to offer to tenants, such as VM roles. This typically involves creating artifacts such as VHDs in the tenant share of the VMM library, configuring Gallery items, and configuring the management portal for administrators to offer the service.
- 2 Create plans (with quotas) and add-ons to bundle the services that you want to offer as a subscription.
- 3 Make plans private or public as needed.
- 4 Manage tenants and resources, and monitor usage.

To learn about general administration of Windows Azure Pack, see the following resources on the web.

- [Administer Plans and Add-ons](http://technet.microsoft.com/library/dn469339.aspx) (http://technet.microsoft.com/library/dn469339.aspx)
- [Administer user accounts and subscriptions](http://technet.microsoft.com/en-us/library/dn249517.aspx) (http://technet.microsoft.com/en-us/library/dn249517.aspx)
- [Windows Azure Pack for Windows Server](http://technet.microsoft.com/library/dn296435.aspx) (http://technet.microsoft.com/library/dn296435.aspx)
- [The Windows Azure Pack Wiki](http://social.technet.microsoft.com/wiki/contents/articles/20689.the-windows-azure-pack-wiki-wapack.aspx) (http://social.technet.microsoft.com/wiki/contents/articles/20689.the-windows-azure-pack-wiki-wapack.aspx)
- [Provision and configure services in Windows Azure Pack](http://technet.microsoft.com/library/dn457759.aspx) (http://technet.microsoft.com/library/dn457759.aspx)
- [Virtual Machine Clouds troubleshooting](http://technet.microsoft.com/library/dn554317.aspx) (http://technet.microsoft.com/library/dn554317.aspx)
- [Troubleshooting Windows Azure Pack & Gallery Items \(VM Roles\) \(Part 1\)](https://blogs.technet.microsoft.com/privatecloud/2013/11/24/troubleshooting-windows-azure-pack-gallery-items-vm-roles-part-1/) (https://blogs.technet.microsoft.com/privatecloud/2013/11/24/troubleshooting-windows-azure-pack-gallery-items-vm-roles-part-1/)
- [Troubleshooting Windows Azure Pack & Gallery Items \(VM Roles\) \(Part 2\)](http://blogs.technet.com/b/privatecloud/archive/2013/11/25/troubleshooting-windows-azure-pack-amp-gallery-items-vm-roles-part-2.aspx) (http://blogs.technet.com/b/privatecloud/archive/2013/11/25/troubleshooting-windows-azure-pack-amp-gallery-items-vm-roles-part-2.aspx)

Walkthrough: Deploying a stand-alone VM using the TenantPlan

The following outlines steps to take when deploying a VM with the **TenantPlan**.

Viewing and updating plan settings

To view and update the **TenantPlan** settings:

- 1 In the Windows Azure Pack management portal for administrators, click **Plans**.
- 2 Click **TenantPlan**.
- 3 Under **Plan services**, click **Virtual Machine Clouds**.
- 4 Scroll down the page to view the resources that are available to the plan. By default, several VM templates that map to Azure sizing (except for storage) are available.
- 5 Under **Networks**, click **Add networks**. Select the check box for each tenant VM network that you want to add to the plan.

NOTE: If the Management VM network is listed, remove it. If you see this VM network listed, make sure you have completed the steps in [Adding tenant VM networks to the cloud](#).

- 6 Click **Save**.

Enabling Remote Desktop in the default VM templates—optional

By default, Remote Desktop is not enabled in the operating system images that are used by the default VM templates. If you want to enable Remote Desktop in the templates, you can use an answer file—`Unattend.xml` file.

- 1 On the Console VM, copy the following text to Notepad, and then save the file as `RemoteDesktopUnattend.xml`.

```
<?xml version="1.0" encoding="utf-8"?>

<unattend xmlns="urn:schemas-microsoft-com:unattend">
```



```

<settings pass="specialize">

<component name="Microsoft-Windows-TerminalServices-LocalSessionManager"
processorArchitecture="amd64" publicKeyToken="31bf3856ad364e35" language="neutral"
versionScope="nonSxS" xmlns:wcm="http://schemas.microsoft.com/WMIConfig/2002/State"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

<fDenyTSConnections>>false</fDenyTSConnections>

</component>

<component name="Networking-MPSSVC-Svc" processorArchitecture="amd64"
publicKeyToken="31bf3856ad364e35" language="neutral" versionScope="nonSxS" xmlns:wcm="http://
schemas.microsoft.com/WMIConfig/2002/State" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">

<FirewallGroups>

<FirewallGroup wcm:action="add" wcm:keyValue="1">

<Group>@FirewallAPI.dll,-28752</Group>

<Profile>all</Profile>

<Active>>true</Active>

</FirewallGroup>

</FirewallGroups>

</component>

</settings>

```

- 2 Copy the RemoteDesktopUnattend.xml file to the VMM library:
 - a In the VMM console, open the **Library** workspace.
 - b Under **Library Servers**, under the library server name, right-click the library share (**MSSCVMLibrary**), and then click **Explore**.
 - c You can drag and drop the **.xml** file to the share.
- 3 Refresh the library share. Right-click **MSSCVMLibrary**, and then click **Refresh**.
- 4 In the **Physical Library Objects** pane, make sure the **.xml** file is listed. If it is not listed, make sure the file extension is correct, and that it was not saved as a **.txt** file.
- 5 In the navigation tree, under **Templates**, click **VM Templates**
- 6 Configure a template to use the RemoteDesktopUnattend.xml file.
 - a Right-click the template, and then click **Properties**.
 - b Click the **OS Configuration** tab.
 - c Under **Scripts**, click **Answer File**.
 - d Click **Browse**, click the **RemoteDesktopUnattend.xml** file, and then click **OK**.
 - e Click **Yes** when prompted if you want to populate the OS profile, and then click **OK**.
- 7 Repeat the previous step for each template that you want to modify.

Subscribing to the plan and deploying a VM

To subscribe to a plan and deploy a VM:

- 1 Open the Windows Azure Pack management portal for tenants.
- 2 If prompted, click **Continue to this website (not recommended)**. You may have to click this two times.
- 3 On the **Login** page, click **Sign Up**.

4 Enter your email address, specify a password, and then click **Sign up**.

NOTE: If you have not yet changed the authentication method for the Windows Azure Pack management portal for tenants, you can sign in by using any email account. After you change the authentication method, you must use an account from a federated domain.

5 Under **New**, click **My account**, and then click **Add subscription**.

6 By default, **TenantPlan** is listed. Click the checkmark to subscribe to the plan.

7 Click **New**, click **Standalone Virtual Machine**, and then click **From Gallery**.

NOTE: If you click **Quick Create**, it will not work unless you change the VM network that is associated with the network adapter in the VM template in the Library workspace of VMM. The **Quick Create** option does not enable you to select the VM network to use, or to specify a product key.

8 Select a template, and then click the **Next** arrow.

9 Enter a name for the VM, the administrator password for the VM, and the product key. You can use the key for Windows Server 2012 R2 Datacenter from the [Automatic Virtual Machine Activation](#) TechNet website. (See the "AVMA keys" section.)

10 For **Network Adapter 1**, choose the VM network, and then click the check mark.

11 Wait for the VM to provision.

When it is ready, the VM should have a status of **Running**.

all items

NAME	TYPE	STATUS	SUBSCRIPTION	
MyTestVM	Standalone	Running	TenantPlan	

Figure 12. VM status

12 By default, Remote Desktop is not enabled in the images that are used by the default templates. If you did not enable it through an answer file, you can do any of the following to connect to the VM:

- You can administer the VM by using a remote Windows Power Shell session.
- You can configure Remote Console access, as discussed in the following section.
- If a VMM administrator knows the administrator name and password that was specified for the VM, you can connect to the VM in the VMM console, and enable Remote Desktop. In the VMM console, in the **VMs and Services** workspace, right-click the **VM**, point to **Connect or View**, and then click **Connect via Console**. After you are connected to the VM, enable Remote Desktop in Server Manager.

NOTE: If it is a Core image, you can use the instructions in this blog post: http://blogs.technet.com/b/bruce_adamczak/archive/2013/02/12/windows-2012-core-survival-guide-remote-desktop.aspx.

13 If Remote Desktop is enabled for the image, you can connect to the VM either from the tenant portal, or through a direct Remote Desktop Connection. Realize that you need to connect from a network that can reach the tenant VM network on which the VM is deployed:

- To connect through the tenant portal, in the navigation pane, click **Virtual Machines**. With the VM that you want selected, click **Connect**, and then click **Desktop**. Click the check mark, click **Open** to open the **.rdp** file, and then click **Connect**.

NOTE: If there are multiple VMs, click inside the row to select the VM; but not the VM name. If you do click the VM name, this takes you to a dashboard for the VM. You can also connect from here.

- To find the IP address to use for an RDP session when you do not want to use the portal, you can view and note this information when you click **Connect**, and then **Desktop** in the portal. Or, you can click **Virtual Machines**, and then click the name of the VM. Click **Dashboard** and then, under **Quick Glance**, locate the IP address.

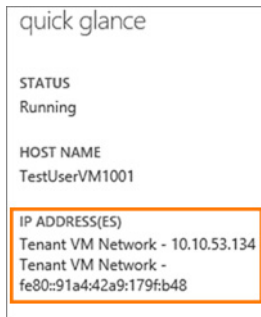


Figure 13. IP addresses

Required settings if you want to create your own VM templates

If you create your own VM templates in VMM, be aware that the following settings are required for Azure Site Recovery to work correctly.

NOTE: You can open the Create VM Template Wizard from the Library workspace in the VMM console. Under Templates, right-click VM Templates, and then click Create VM Template.

Use the following settings with the Create VM Template Wizard:

- 1 On the **Identity** page of the wizard:
 - a For **Generation**, select **Generation 1**.

NOTE: This setting appears only if you specify a virtual hard disk as the source.
- 2 On the **Configure Hardware** page:
 - a Under **Network Adapters**, you must have a network adapter that is connected to a VM network.
 - b Under **Bus Configuration**, make sure that one disk has the **Contains the operating system for the virtual machine** check box selected.
 - c Under **Advanced**, mark the VM as highly available. Click **Availability**, and then select the **Make this virtual machine highly available** check box.
- 3 On the **Configure Operating System** page:
 - a In the **Guest OS profile** list, select **Create new Windows operating system customization settings**.
 - b For **Operating System**, make sure that you select the operating system of the virtual machine.
- 4 On the **Application Configuration** page:
 - a For **OS Compatibility**, make sure that you select the operating system of the virtual machine.

Managing tenants

The Windows Azure Pack management portal for administrators gives you the ability to manage both tenants and subscriptions. You can create, delete, suspend, or otherwise make changes to tenant accounts or subscriptions.

For additional information, see [Administer User Accounts and Subscriptions](http://technet.microsoft.com/library/dn249517.aspx) (<http://technet.microsoft.com/library/dn249517.aspx>) in the Microsoft TechNet Library.

User Accounts Page

On the **User Accounts** page, you can see a list of tenants, including:

- When they are active
- When they enrolled
- Their numbers of subscriptions

You can also search for subscriptions, and suspend and delete user accounts.

Click a user name to see the subscriptions for a tenant. On this page, you can do the following:

- Add subscriptions to an account.
- Click a subscription name to get more details about the subscription, such as status and usage data.

If you click a subscription, you see information similar to the following:

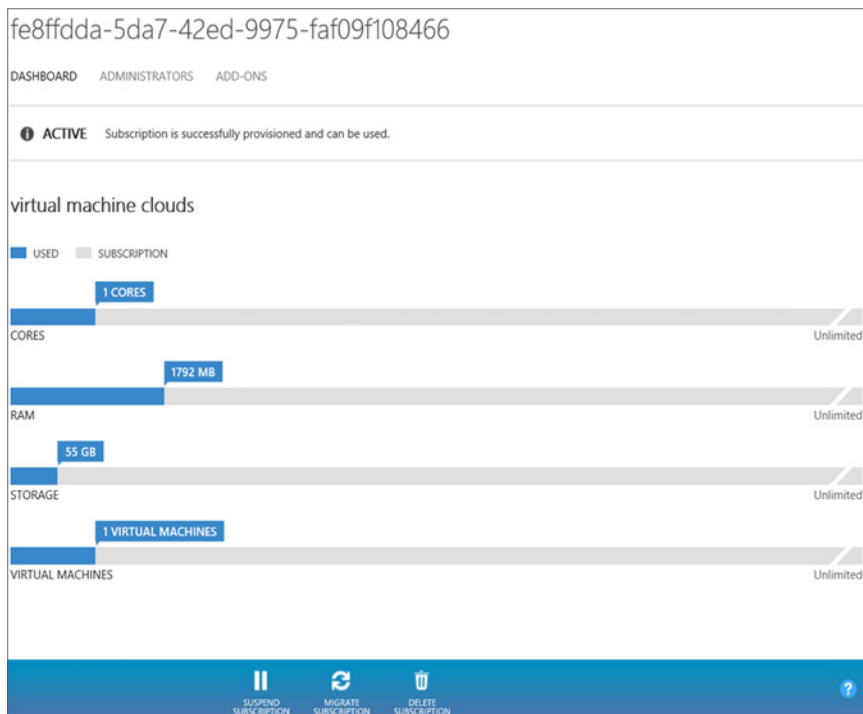


Figure 14. Subscription details

On this page you can:

- **Suspend, migrate, and delete subscriptions**—You can manage each subscription separately.
- **Manage administrators**—You can add coadministrators to allow teams to share a subscription. This addition can be helpful for development operations, where everyone can have tenant administrative access to a subscription.
- **Manage plan add-ons**—Users can add add-ons to their subscriptions, and you can manage them here.

Managing subscriptions

A subscription is created when a tenant signs up for a plan.

Each tenant account can have multiple subscriptions. Each subscription is associated with just one plan. Administrators can migrate and delete subscriptions.

You can use the plan dashboards to easily see the number of subscribers to a plan. To open a plan dashboard, click **Plans** in the navigation pane, and then click a plan in the list.

Deleting subscriptions

To delete a subscription, all of the resources created in that subscription must be deleted. You can do this in the management portal for administrators.

- 1 Identify the user ID of the user whose subscriptions need to be deleted.
- 2 In the management portal for administrators, click **Plans**, and then click **Subscriptions**.
- 3 Search for the user ID in the **Search** bar to display a list of subscriptions that are associated with the user ID.
- 4 Select the subscription, and then click **Delete Subscription** on the menu bar.

- 5 Confirm the deletion.
- 6 The subscription, and the resources associated with the subscription, are deleted.

Monitoring capacity

To ensure high-availability for your plans and services and help keep your tenants productive, you need to monitor the performance of your resources.

Dell Hybrid Cloud System for Microsoft uses Operations Manager and Operational Insights to monitor the health of your cloud infrastructure. See the [Operations](#) chapter of this guide for more information.

Activating guest operating systems

By default, tenant VMs that are running Windows Server 2012 R2 are automatically activated by using Automatic Virtual Machine Activation (AVMA), if an AVMA key was used. For more information about AVMA, including the AVMA keys that you should use for tenants in VM templates for Windows Server 2012 R2-based images, see [Automatic Virtual Machine Activation](http://technet.microsoft.com/library/dn303421.aspx) (<http://technet.microsoft.com/library/dn303421.aspx>) in the Microsoft TechNet Library.

If you want to offer tenants the option of deploying earlier Windows-based operating systems, you must use a Windows Server Key Management Server (KMS) to activate those products. If you already have a KMS server, you can use the existing server.

To set up a KMS host in your environment, see the blog post [Installing Volume Activation Services Role in Windows Server 2012 to set up a KMS Host](http://blogs.technet.com/b/askcore/archive/2013/03/14/installing-volume-activation-services-role-in-windows-server-2012-to-setup-a-kms-host.aspx) (<http://blogs.technet.com/b/askcore/archive/2013/03/14/installing-volume-activation-services-role-in-windows-server-2012-to-setup-a-kms-host.aspx>).

NOTE: The same steps apply to Windows Server 2012 R2.

Keep in mind that if a tenant does not connect the VM network to a gateway, for example in an isolated development environment, the VM is not able to reach the KMS server because the VM cannot reach the internet. In this scenario, there are the following options:

- Use a volume licensed version of the operating system in the image.
- Specify the KMS Client Key in the VM template. For a list of KMS client keys, see [Appendix A: KMS Client Setup Keys](http://technet.microsoft.com/en-us/library/jj612867.aspx) (<http://technet.microsoft.com/en-us/library/jj612867.aspx>).

VM template requirements (pre-Windows Server 2012 R2)

If you create pre-Windows 2012 R2 images to use in VM templates for tenant use, you must do the following:

- Use a volume licensed version of the operating system in the image.
- Specify the KMS Client Key in the VM template. For a list of KMS client keys, see [Appendix A: KMS Client Setup Keys](http://technet.microsoft.com/en-us/library/jj612867.aspx) (<http://technet.microsoft.com/en-us/library/jj612867.aspx>).

Optional configuration

The following procedures are optional.

Customizing the tenant portal

For information about how to customize the Windows Azure Pack management portal for tenants, see [Windows Azure Pack custom theming](http://msdn.microsoft.com/library/dn448611.aspx) (<http://msdn.microsoft.com/library/dn448611.aspx>) in the MSDN Library.

Configuring Remote Console access

Remote Console provides tenants with the ability to access the console of their VMs in scenarios when other remote tools such as Remote Desktop are unavailable.

Tenants can use Remote Console to access VMs when the VM is on an isolated network, an untrusted network, or across the Internet. The Remote Desktop Gateway (RD Gateway) component enables you to offer Remote Console to tenants who do not have direct network connectivity to the Hyper-V hosts.

For more information about Remote Console, including an automated deployment method which makes it easier to install, see the Microsoft blog post [Automation of Remote Console deployment for CPS Standard](#).

Automating tasks for efficiency

You can automate many administrative tasks by using SMA.

For more information, see [Service Management Automation](http://technet.microsoft.com/library/dn469260.aspx) (http://technet.microsoft.com/library/dn469260.aspx) in the Microsoft TechNet Library.

If you are a developer, see the [Service Management Automation Developer's Guide](http://msdn.microsoft.com/library/dn688344.aspx) on MSDN (http://msdn.microsoft.com/library/dn688344.aspx).

Windows Azure Pack API reference content for developers

If you are a developer, you can use the following resources to:

- Create custom providers
- Create Windows Azure Pack user interface extensions
- Build custom portals
- Help with automation for both the administrator and the tenant.

Table 14. Resources for developers

Resource	Link
Windows Azure Pack Developer's Kit	http://msdn.microsoft.com/library/dn448665.aspx <ul style="list-style-type: none">• For infrastructure management, see the Windows Azure Pack IaaS Resource Provider section: http://msdn.microsoft.com/library/dn766004.aspx• For information specific to VM Roles, see the VM Roles Tenant Service section: http://msdn.microsoft.com/library/dn502556.aspx.
Blog post about support for VMM service templates in IaaS APIs	Windows Azure Pack, Service Provider Foundation and IaaS API Support for VMM Service Templates

Configuring disaster recovery protection

In Dell Hybrid Cloud System for Microsoft, you can provide disaster recovery protection for tenant VMs with [Azure Site Recovery](#). You can set up protection between a Dell Hybrid Cloud System for Microsoft stamp and Microsoft Azure.

With this configuration, VMs that are located on an on-premises Dell Hybrid Cloud System for Microsoft stamp replicate and fail over to Azure VMs. Replication and failover is orchestrated by Azure Site Recovery. Data is stored in an Azure storage account.

Step 1: Onboard to Azure Site Recovery

You can opt in to Azure Site Recovery only after Dell Hybrid Cloud System for Microsoft deployment has completed. Azure onboarding is not supported during initial deployment.

Pre-requisites:

- Internet access is required. You must have an internet connection available for the solution to use.
- You must have a valid Azure account to a subscription prior to configuring this feature.

If you opted in to Azure Site Recovery during Dell Hybrid Cloud System for Microsoft installation, protection is already enabled for the default plan (**TenantPlan**) in Windows Azure Pack.

Follow these steps at any time after the deployment has completed. You then need to opt in to connect to Azure services.

To onboard to Azure Site Recovery after initial deployment:

NOTE: You need an active Azure subscription for the region in which you are deploying. For instance, a US-based Azure subscription may not show EMEA or APJ regions, and vice versa. Ensure with the customer that the credentials that they have provided are for an active Azure subscription and local to the region in which they want to onboard. Any credentials given must have an Azure subscription tied to them.

- 1 RDP to **<Prefix>CON01** with domain credentials (such as, a member of **<Prefix>-Setup-Admins**).
- 2 Launch the Deployment UI (Dell Hybrid Cloud System for Microsoft).

The UI recognizes that initial deployment has completed, and requests your Active Directory information.

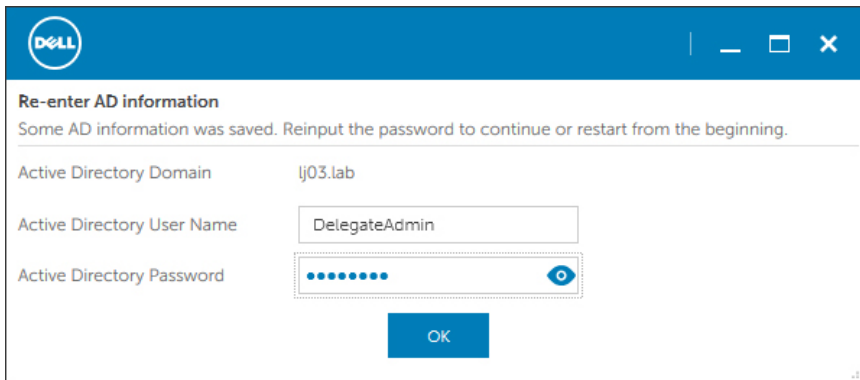


Figure 15. Re-enter AD information

- 3 Re-enter your AD information and click **OK**.
The Proxy information dialog opens.
- 4 Select **Secured Proxy** from the **Proxy Type** drop-down. Enter proxy information, select **Save Credentials**, and then click **OK**.

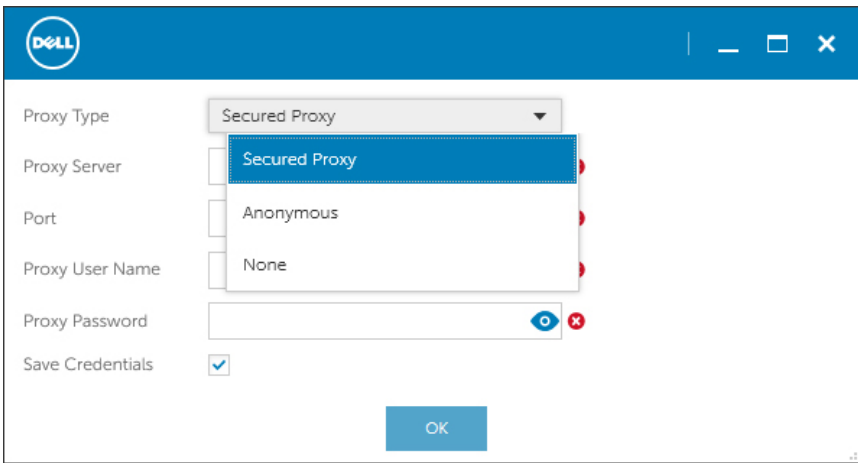


Figure 16. Proxy information

- 5 The Dell Hybrid Cloud System for Microsoft CPS Standard wizard appears. Click **Configure Azure** at the top of the page to start the Azure Onboarding process.

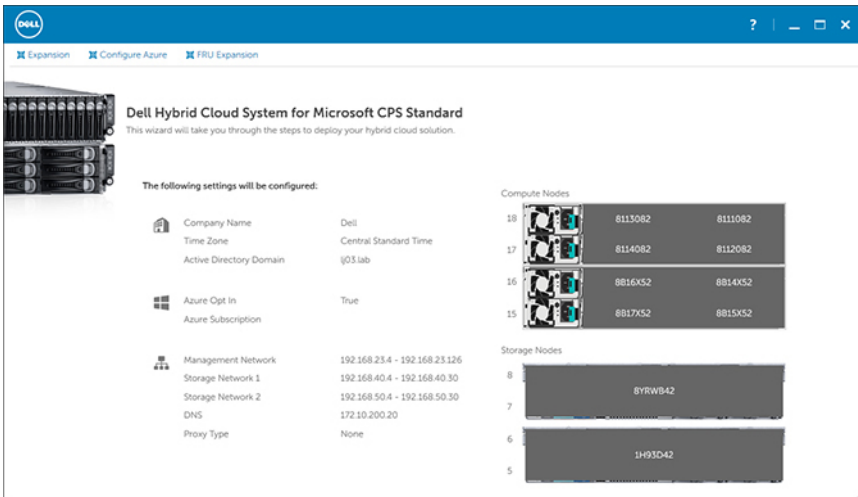


Figure 17. DHCS wizard

- 6 Once the Microsoft server is reached, a window appears for **Azure Login**. Click **Sign In**.

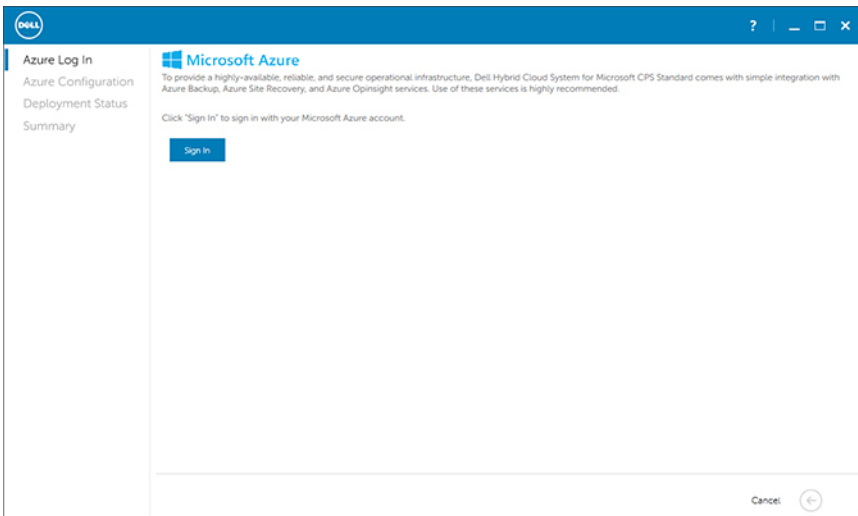


Figure 18. Azure Log In

A few different dialogs may appear, depending on the type of credentials provided. The sign-in dialog on your system may differ from the image that follows.

- 7 Follow the prompts to sign in to Azure. Microsoft validates the username twice so you may be prompted to re-enter your password.

NOTE: It may take up to two minutes for the Sign in dialog to appear.

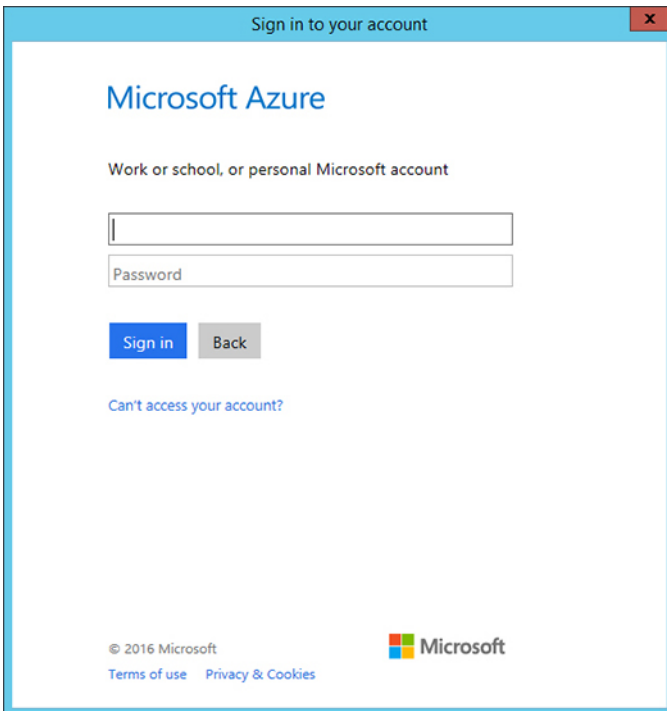


Figure 19. Sign in to Azure

The **Azure Configuration** page appears.

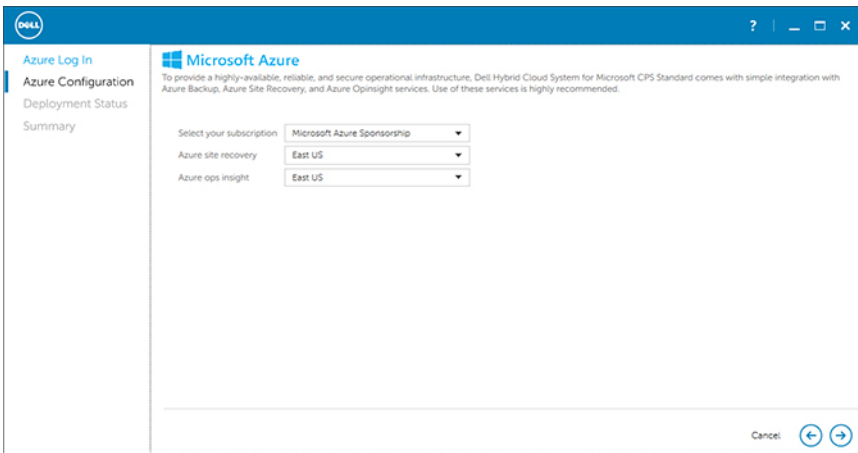


Figure 20. Azure Configuration

- On the **Azure Configuration** page, select the subscription type and the Azure regions into which you want to configure Azure Site Recovery and Azure Operational Insights services.

NOTE: The Microsoft Azure Site Recovery regions that the UI populates are an intersection of Azure Site Recovery, Compute, and Storage regions that are allowed for by the provided subscription. Thus, if the subscription allows for multiple ASR regions, but the Compute and Storage are limited to a subset of regions, the UI only shows the subset of available regions.

- The onboarding process begins. A screen displays output from the configuration scripts that are running to complete the process.

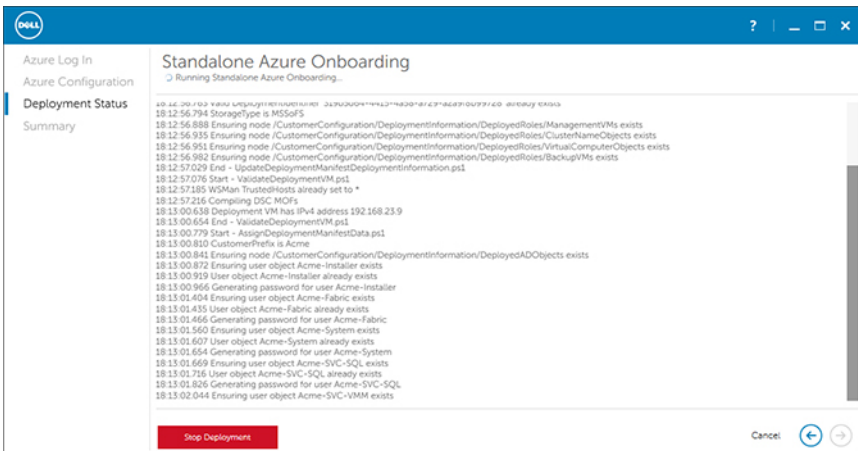


Figure 21. Azure Onboarding begins

CAUTION: Because Azure is a public service, you may encounter connectivity or other issues. If you encounter any issues or failures, see Microsoft Azure Documentation.

If you encounter an error where MapCloud Job fails, rerun the deployment.

- When the process completes, a window appears telling you that deployment has succeeded.

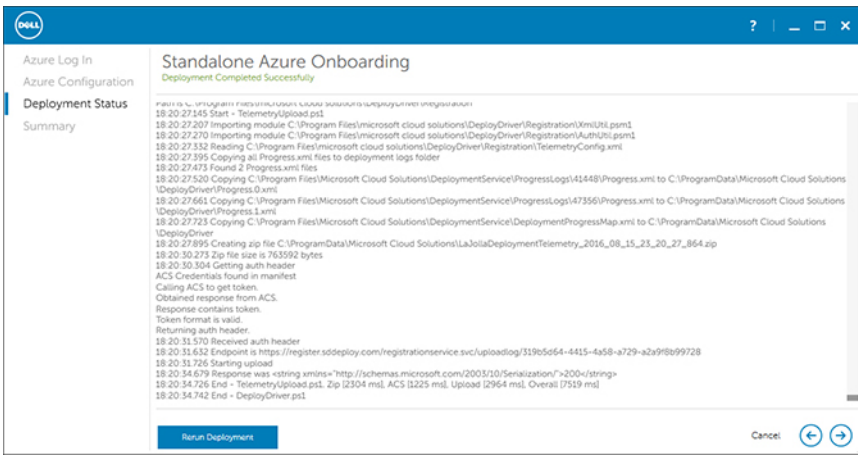


Figure 22. Onboarding complete

11 Notice that the **Summary** opens, telling you that your deployment was successful.

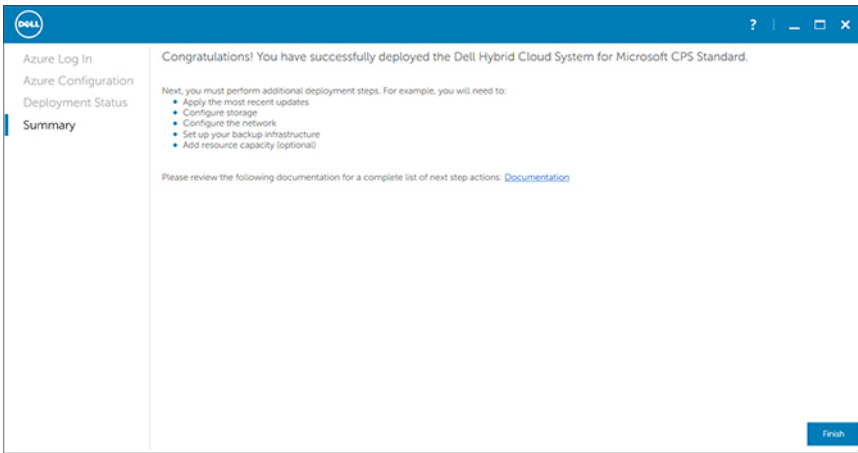


Figure 23. Deployment successful

12 The **Restart** window pops up and prompts you to restart the machine to finish deployment. Click **Yes**.

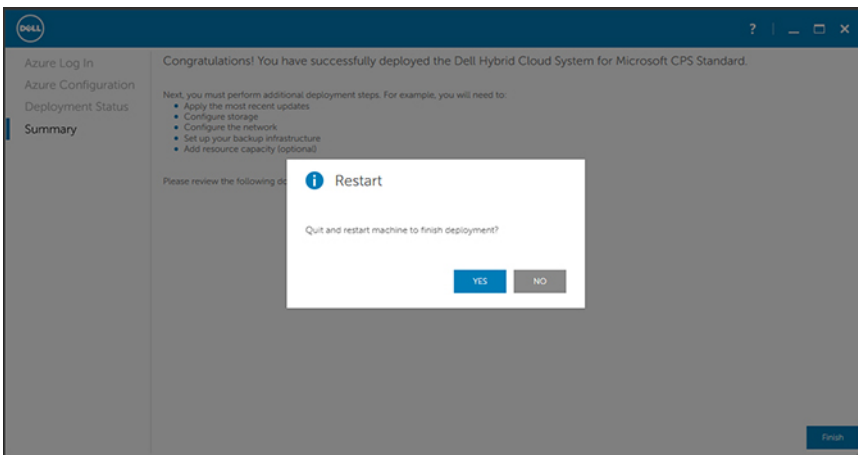


Figure 24. Restart

NOTE: If you deploy the DPM backup infrastructure, and then later onboard to Azure Site Recovery, you see the following error in the Microsoft Azure portal during the onboarding process.

Protection couldn't be configured for cloud/site '<CloudName>'. (Error code: 10003)

Provider error: The Microsoft Azure Recovery Services Agent isn't installed on the Hyper-V host server '<BackupHostName>'. The agent isn't installed.

Install the agent (<https://go.microsoft.com/fwlink/?LinkID=399336>) on the server. (Provider error code: 31313)

Possible causes: One or more hosts couldn't be prepared. Check the Provider error for more information.

Recommendation: Resolve the issue and retry the operation.

You can safely ignore this message. This issue does not affect Azure Site Recovery operations.

The default replication policy settings are summarized in the following table.

Table 15. Default replication policy settings

Setting	Description	Default Value
Encrypt data stored on Azure	Specifies whether replicated data that is transferred should be stored as encrypted.	False
Copy frequency	Specifies how frequently data should be synchronized between Dell Hybrid Cloud System for Microsoft and Azure.	5 minutes
Recovery point retention in hours	Specifies how many hours of recovery history should be stored. With a default value of zero (0), only the latest recovery point for a primary virtual machine is stored.	0
App-consistent snapshot frequency in hours	Specifies how often to create application-consistent snapshots by using Volume Shadow Copy Service (VSS).	0
Initial replication start time	Specifies when the initial replication should start. If you already have tenant workloads when you onboard to Azure Site Recovery, Dell recommends that you schedule network replication during off-peak hours.	Immediately

Step 2: Enable protection on a plan or add-on

By default, the plan called **TenantPlan** has protection enabled after you onboard to Azure Site Recovery.

If you only have the one **TenantPlan**, you can skip this step for now.

If you create more plans or add-ons, you need to configure protection. To enable protection on a published plan or add-on:

- 1 Open the Windows Azure Pack management portal for administrators.
- 2 Click **Plans**.
- 3 On the **Plans** tab, open the relevant plan or open the add-on on the **Add-Ons** tab.
- 4 In **Plan Services** or **Add-On Services**, click **Virtual Machine Clouds**.
- 5 Under **Custom Settings** select the **Enable protection for all virtual machines** check box.

NOTE: The runbook `Invoke-AzureSiteRecoveryManageVmProtectionJob.ps1` detects subscriptions for plans or add-ons that have protection enabled, and then enables protection for VMs in those subscriptions. This happens automatically in accordance with master runbook scheduling. You do not need to take further action.

Step 3: Tenants create resources

To set up VM protection, tenants need to do the following in the Windows Azure Pack management portal for tenants:

- 1 **Subscribe to the plan or add-on**—Tenants subscribe to a plan or add-on that has VM protection enabled.
- 2 **Create a virtual machine**—Under the plan subscription, tenants create a VM or VM role on the Dell Hybrid Cloud System for Microsoft stamp. The VM is created on the associated VMM cloud. The VM owner name is the name of the user who created the VM.

Step 4: Configure network mapping

You can set up network mapping to map VM networks on the VMM server to Azure virtual networks. These mappings indicate how replica VMs will be connected after failover. If a failover occurs, all VMs on the same Azure network can connect to each other. Multiple VM networks on VMM can be mapped to a single Azure network. To do network mapping:

- 1 In the Microsoft Azure portal, <https://portal.azure.com>, create an Azure network with the same subnet settings as the VM network on the on-premises VMM server. For **Resource Group**, use an existing group, or create a resource group.
For more information, see [Create a virtual network using the Azure portal](#) in the Azure documentation. You do not have to add a second subnet as described in the article.
- 2 Go to **Recovery Services vaults**, and then click the name of the vault for the Dell Hybrid Cloud System for Microsoft deployment. Look for `<Prefix>-<DellHybridCloudforMSDeploymentGUID>`. The naming convention may vary based on the update version of the DHCS stamp when onboarding was performed. Check the Release Notes for more information.

TIP: Click **Browse**, locate **Recovery Services vaults** in the list, and then click the star icon to add this feature to the left navigation pane.

The vault dashboard is displayed.

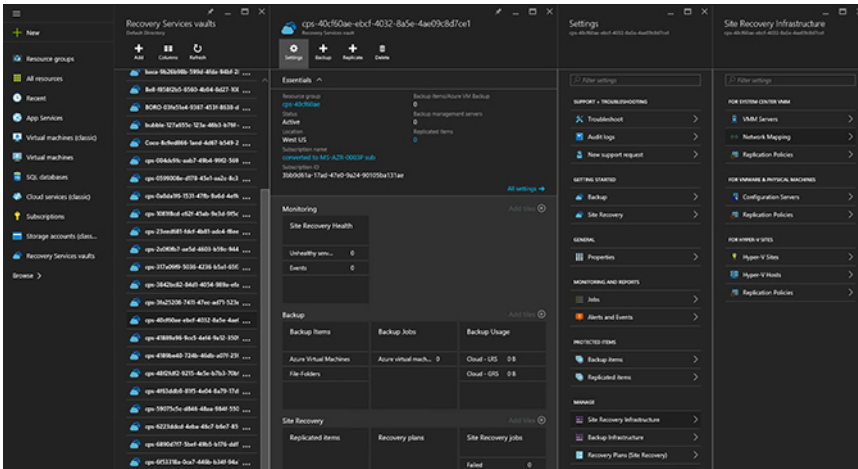


Figure 25. Recovery Services vaults

- 3 In **Settings**, under **Manage**, click **Site Recovery Infrastructure**.
- 4 In **Site Recovery Infrastructure**, under **For System Center VMM**, click **Network Mapping**.
- 5 In the **Network Mapping** blade, click **Network Mapping**.
- 6 In the **Add network mapping** blade:

- a Under **Source VMM**, select the source VMM server (<Prefix>VMM01).
- b Under **Source network**, select the virtual network on the VMM server that you want to map.
- c Under **Target**, click **Azure**.
- d Under **Subscription**, choose the appropriate subscription.
- e Under **Compute stack**, click **Resource Management**.
- f Under **Target network**, the service detects the VM networks on the target location and lists them. Choose the appropriate target network, as identified in Step 1 of this procedure, and then click **OK**.

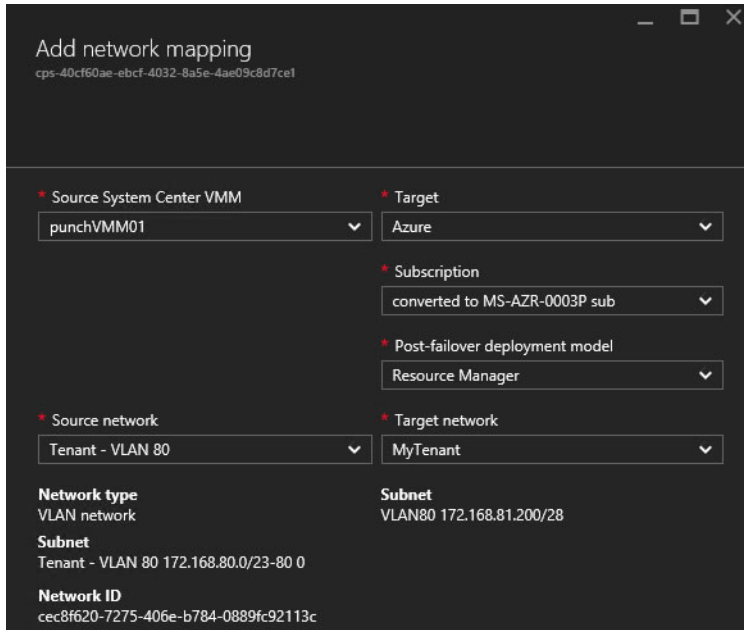


Figure 26. Add network mapping

This step triggers a job.

- g To track the progress of the job triggered in the previous step, click **Settings**. Under **Monitoring and reports**, click **Jobs**.
- h In **Jobs**, under **General**, click **Site Recovery jobs**.

Step 5: Run a failover

After the initial replication, you can run failovers as desired. The three types of failovers are:

- Test
- Planned
- Unplanned

You can run failovers as follows:

- 1 **Test failover**—Run to verify the environment without having any impact on the production infrastructure. You can run a test failover if the tenant requests it. Run a test failover as follows:
 - a In the Azure portal, create a separate virtual network for test purposes. Use the same subnet settings as the VM network which your test VM is connected to on the VMM server.
 - b In **Recovery Services vaults**, click the name of the vault for the Dell Hybrid Cloud System for Microsoft deployment.
 - c In **Settings**, under **Protected Items**, click **Replicated items**.
 - d Click the **VM** that you want to fail over.
 - e Click **Test Failover**.

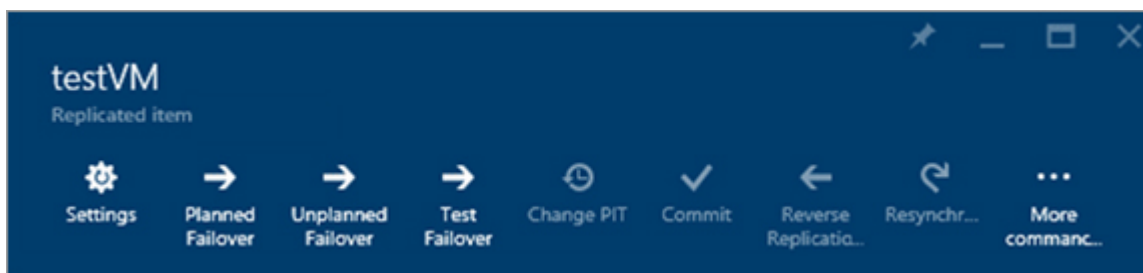


Figure 27. Test failover commands

- f Under **Azure virtual network**, select the virtual network that you created in the first step of this procedure, and then click **OK**.

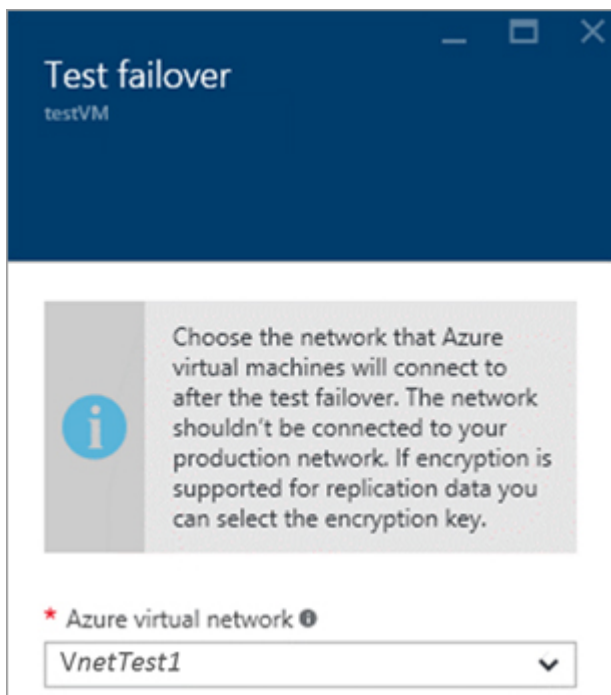


Figure 28. Choosing the network

This step triggers a job.

- g To track the progress of the job triggered in the previous step, click **Settings**. Under **Monitoring and reports**, click **Site Recovery jobs**.

Test failover creates an Azure IaaS virtual machine that corresponds to the VM on the VMM server. You can access and test this VM from the Azure portal. To learn more about Azure IaaS VMs, see [Create a Windows virtual machine in the Azure portal](#) in the Azure documentation.

- h After you verify that the test failover was successful and that the test VM was replicated in Azure, click **Complete Test** to finish the test. This deletes the replicated VM in Azure.

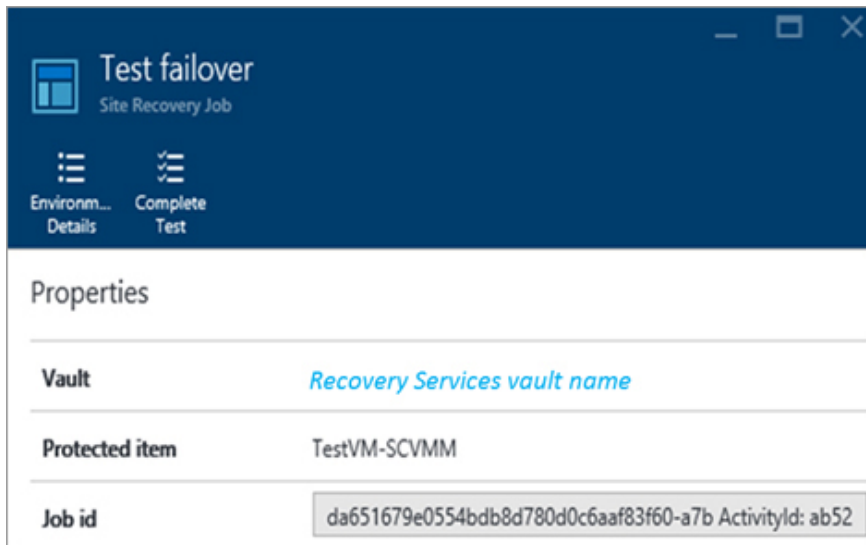


Figure 29. Completing the test failover

- 2 **Planned failover**—Run for planned maintenance. Run a planned failover as follows:
 - a In the Azure portal, open **Recovery Services vaults**, and then click the name of the vault for the Dell Hybrid Cloud System for Microsoft deployment.
 - b In **Settings**, under **Protected items**, click **Replicated items**.
 - c Click the **VM** that you want to fail over, and then click **Planned Failover**.
 - d Verify the failover direction, and then click **OK**.

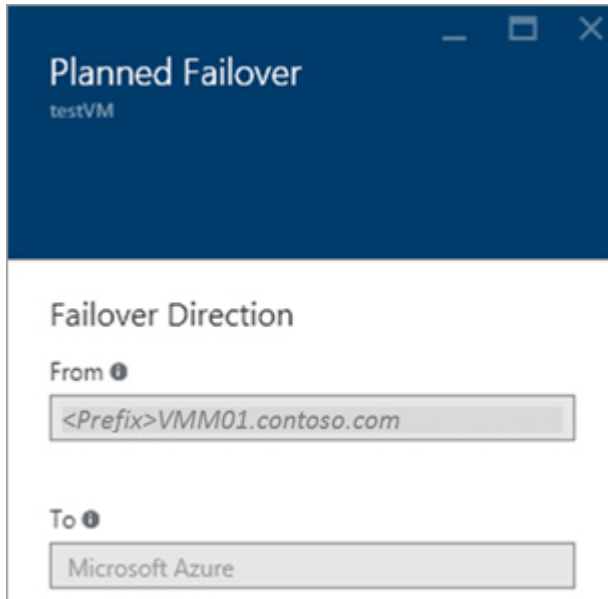


Figure 30. Planned failover direction

This step triggers a job.

- e To track the progress of the job triggered in the previous step, click **Settings**. Then, under **Monitoring and reports**, click **Site Recovery jobs**.
- 3 **Unplanned failover**—Run for disaster recovery after unplanned maintenance or downtimes. Run an unplanned failover as follows:
 - a In the Azure portal, open **Recovery Services vaults**, and then click the name of the vault for the Dell Hybrid Cloud System for Microsoft deployment.

- b Open **Settings**. Under **Protected Items**, click **Replicated items**.
- c Click the **VM** you want to fail over, and then click **Unplanned Failover**.
- d Verify the failover direction. If desired, select the **Shut down the virtual machine** check box. Click **OK**.
This step triggers a job.
- e To track the progress of the job triggered in the previous step, click **Settings**. Then, under **Monitoring and reports**, click **Site Recovery jobs**.

Step 6: Access replicated VMs

Failover with Azure Site Recovery creates the replica VM in Azure. After failover, the service administrator can sign in to the Azure portal using personal credentials, and access the replica VMs from the portal. The administrator can then configure application and RDP ports on the VMs to provide tenant access. If tenants access VMs in the data center over a virtual private network (VPN) connection, you must set up VPN connectivity between the tenant location and Azure so tenants can also access the replicated VMs over VPN.

To configure ports on the VMs, you must configure the subnet for the Azure virtual network to use a network security group (NSG). Do the following:

- 1 First, create an NSG with the appropriate port rules.
- 2 Then, in the settings for the virtual network, go to the subnet settings, and associate the NSG.

For more information about NSGs, see [How to manage NSGs using the Azure portal](#) in the Azure documentation.

Operations

This chapter discusses how you can monitor system health using the Operations Manager.

Topics:

- [Monitoring](#)
- [Backup and recovery](#)
- [Updating the Dell Hybrid Cloud System for Microsoft](#)
- [Shutting down and starting up the stamp](#)

Monitoring

By default, you can use Operations Manager to monitor the health of the system.

Any member of the group **<Prefix>-Ops-Admins** can connect to the Operations console.

If you opt in to Azure services, you can also use Operational Insights. Operational Insights is also known as Microsoft Office Management Suite (OMS), a cloud-based IT management solution.

Onboarding to Operational Insights

You can opt in to Azure services during Dell Hybrid Cloud System for Microsoft deployment, or at any time after deployment by using the Operational Insights wizard.

When you opt in to Azure services, onboarding to Operational Insights occurs automatically. For information about the OMS suite, go to <http://microsoft.com/oms>.

By default:

- Operational Insights is configured to use the Operations Manager instance on the Dell Hybrid Cloud System stamp as the data source.
- A workspace is created. The workspace is a logical container for storing your management data.
- Several solutions are pre-selected for your implementation.

To sign in to Operational Insights, go to <http://microsoft.com/oms>. Sign in by using your Azure subscription for the Dell Hybrid Cloud System for Microsoft stamp.

You can also configure Operational Insights to collect log information and other data, such as Windows event logs and performance counters. For more information, see "Add logs and machine data" at <https://technet.microsoft.com/library/mt679065.aspx>. To enable log collection:

- 1 Sign in to Operational Insights.
- 2 Select the **Get started** tile.
- 3 Click **Add logs**.
- 4 Enable logging as needed.

For information about how to use Operational Insights, see the OMS TechNet Library site, at <https://technet.microsoft.com/library/mt484091.aspx>.

Using Operations Manager

From the **Monitoring** workspace in Operations Manager, you can view the health of the Dell Hybrid Cloud System for Microsoft stamp and its components.

Take time to familiarize yourself with what information is available in the various views and dashboards. For example, under **Monitoring**, you can click **Active Alerts** to view all active alerts.

To view the health of the Dell Hybrid Cloud System for Microsoft stamp, the best place to look is the Microsoft Cloud Dashboard.

Using the Microsoft Cloud Dashboard

In Operations Manager, the Microsoft Cloud Dashboard lets you quickly see whether any issues require your attention. This dashboard consolidates health state and alerting views for:

- Compute—Hyper-V hosts
- Storage
- Management Services—the infrastructure VMs
- Backup
- Antimalware
- Tenant VMs

After you see the health state roll-up views, you can dig deeper by clicking individual tiles.

To access the dashboard:

- 1 Open the Operations Console.
- 2 In the **Monitoring** workspace, expand **Microsoft Cloud Dashboard**, and then click **Microsoft Cloud Dashboard**.

The dashboard displays a set of tiles. This display provides you with a quick view of system health. Each tile shows the number of alerts and the health state.

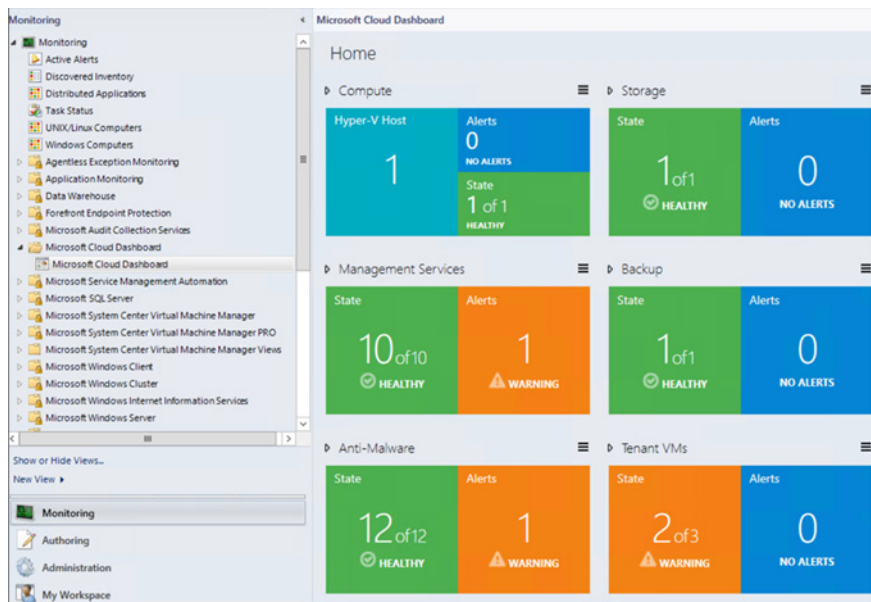


Figure 31. Microsoft Cloud Dashboard

To drill down further and view specific alert details, or to access a list of tasks and views, double-click a tile. You can continue to double-click items to drill down further to view the health.

For example:

- 1 If you double-click the **Compute** tile, you see a list of all compute nodes, and their overall health.
- 2 You can click one of the nodes, and run several tasks against the node from here. For example, in the **Tasks** pane, in the **Object Tasks** section, there is a long list of operations that you can perform against the node. For example, for a compute node, you can display the local users, the network shares, the IP address information, ping the computer, and start a Remote Desktop session.
- 3 You can double-click a compute node to drill down further and view alerts.
- 4 You can then double-click an active alert to view the alert information.

Management packs that are imported by default

By default, Dell Hybrid Cloud System for Microsoft setup automatically imports several management packs that apply to your cloud infrastructure. To view the management packs, in the Operations console, open the **Administration** workspace, and then click **Management Packs**.

Getting started with monitoring

Before you begin monitoring:

- Make sure the state of all computers is understood.
- Take care of any actions needed to get to all computers green.
- Make sure no rule-based-alerts need action, and then close them.

Setting up notifications for critical alerts

When a critical alert occurs, it is important to know about it. In System Center 2012 R2– Operations Manager, when an alert is generated, Operations Manager can notify designated individuals by email, instant message (IM), or text message (SMS). Notifications can also run commands automatically when an alert is raised on a monitored system.

Notifications have these elements:

- A Run As account that provides credentials to the Notification Account Run As profile. If your SMTP is configured to only support sending email from authenticated accounts, then the domain Dell Hybrid Cloud System for Microsoft is using must have two-way trust with the domain of the SMTP server.
- A notification channel that defines the format for the notification and the way the notification is sent.
- A notification subscriber that defines the recipients and the schedule for sending notifications to the subscriber.
- A notification subscription that defines the criteria for sending a notification, the channel to be used, and the subscribers to receive the notification.

An Operations Manager administrator must configure the Run As account for notifications and define the notification channels. An Operations Manager administrator, advanced operator, or operator can create a subscriber and a subscription.

For more information, see [Subscribing to Alert Notifications](#) in Microsoft TechNet.

Recovering from an alert storm

Many alerts, known as an *alert storm*, can occur if there is:

- An incident such as a power outage, or
- Disruptive maintenance, where maintenance mode was either not used or not effective because of wide-spread impact.

The recommended response is to do the following:

- Resolve rule-based alerts created or not modified since the incident.
 - **NOTE: Do not resolve rule-based alerts on physical disk storage enclosure failures.**
- Investigate remaining alerts and computers with a **Critical** or **Warning** health state.

To resolve rule-based alerts, use the Operations Manager task **Resolve Rule Generated Alerts**:

- 1 In Operations Manager, open the **Monitoring** workspace.
- 2 Expand **Operations Manager > Management Server**, and then click **Management Servers State**.
- 3 In the **Management Server State** pane, click the **Operations Manager** server.
- 4 In the **Tasks** pane, under **Health Service Tasks**, click **Resolve Rule Generated Alerts** to resolve rule-based alerts.

You can also connect to the **<Prefix>OM01** server, through the Operations Manager Shell on the Console VM, and use the following example Windows PowerShell script to resolve rule-based alerts:

```
# Set this to the # of hours back to resolve alerts
$ModifiedOlderThanHours = 10

# Query for the Alerts, review before resolving if you want
$AlertsToResolve = get-scomalert -criteria 'ResolutionState=''0'' AND IsMonitorAlert=''False''
| where {($_.LastModified).ToLocalTime.ToDateTime -le (Get-Date).addhours(-
$ModifiedOlderThanHour) }

# Resolve the Alerts

$AlertsToResolve | resolve-SCOMAlert -Comment 'Close old alerts generated by rules' -PassThru |
Set-SCOMAlert -ResolutionState 255
```

Using Operational Insights

If you did not opt in to Operational Insights during deployment, you can do so at any time by using the Dell Hybrid Cloud System wizard that is used for onboarding to Azure Site Recovery. The instructions for onboarding are listed in [Step 1: Onboard to Azure Site Recovery](#).

For information about Operational Insights, see the [Operational Insights](#) page on the Microsoft Azure site, and the associated [documentation](#).

Backup and recovery

It is very important to protect all of the infrastructure VMs and the tenant VMs.

Dell Hybrid Cloud System for Microsoft uses System Center Data Protection Manager (DPM) for that protection, with the option to also back up from DPM to Microsoft Azure.

Onboard to Azure Backup

If you decided to opt in to Azure Backup after the initial backup infrastructure deployment, you can do so at any time. As a prerequisite, you need an Azure subscription.

Use the following steps to attach the existing DPM servers to Azure:

- 1 On the Console VM, log on as a member of the **<Prefix>-Ops-Admins** group.
- 2 At a command prompt, run the following commands to enable the default local Administrator account, and to make sure that the password is set correctly. For onboarding to Azure Backup, this account must have a specific password assigned.

```
net user administrator /active:yes
net user administrator pass2015@MSPCS
```
- 3 Log off, and then back on to the Console VM as the default local Administrator account with the password `pass2015@MSPCS`.
- 4 You must run a script to onboard to Azure Backup. The following table lists the variable values that you must assign when you run the script. Before you begin, make sure that you have collected the required information.

Parameter Name Description

DomainCredential	The username and password of a member of the <Prefix>-Diag-Admins group. Specify these credentials for <code>\$DomainUserName</code> and <code>\$DomainPassword</code> in the script.
AzureRegion	The region in which the Azure backup vault must be created, for example <i>West US</i> . For a list of regions, see http://azure.microsoft.com/regions/ .
StorageType	The storage type to use for the backup vault. Permitted values are: <ul style="list-style-type: none">• <i>Geo Redundant</i>• <i>Locally Redundant</i> For more information, see https://azure.microsoft.com/documentation/articles/storage-redundancy/ .
Passphrase	An alpha-numeric string of at least 16 characters that is used as an encryption key.

 **NOTE: You must store this key somewhere. You will need it if you ever have to rebuild the DPM server.**

- 5 Open a Windows PowerShell session, and then run the following script. First, replace the variable values.

```
cd "C:\Program Files\Microsoft Cloud Solutions\DeployDriver\BackupDeployDriver"

$DomainUsername = <username>

$DomainPassword = <password>


$DomainCredential = New-Object System.Management.Automation.PSCredential ("$DomainUsername",
(ConvertTo-SecureString -String $DomainPassword -AsPlainText -Force))

$AzureRegion = "<AzureRegion>"

$Passphrase = <Passphrase>

$StorageType = "<StorageType>"

.\BackupAzureOnboarding.ps1 -DomainCredential $DomainCredential -AzureRegion $AzureRegion -
Passphrase $Passphrase -StorageType $StorageType
```
- 6 When prompted for the Azure credentials, enter them, and click **Continue**.
- 7 After this script completes, log off the Console VM, and then log back on using an account that is a member of the **<Prefix>-Ops-Admins** group.

 **NOTE: If you receive an error, see [Troubleshooting "Set-DPMCloudSubscriptionSetting" or "Start-DPMCloudRegistration" errors](#).**
- 8 Open the Windows Azure Pack management portal for administrators, and run the **Protect-ManagementComponents** runbook. This enables online protection for all the management VMs and databases.
- 9 When you are done, disable the local Administrator account on the Console VM. At a command prompt, run the following command:

```
net user administrator /active:no
```

Troubleshooting "Set-DPMCloudSubscriptionSetting" or "Start-DPMCloudRegistration" errors

You may receive either of the following error messages when you run the BackupDeployDriver.ps1 script:

- Set-DPMCloudSubscriptionSetting : The current operation failed due to an internal service error [0x38276]. Please retry the operation after sometime. (ID: 100066)
- Start-DPMCloudRegistration : The service encountered an internal error. (ID: 130043)

Retry the operation after some time. If the issue persists, contact Microsoft Support.

```
At Configure-BackupToAzure:1027 char:1027
```

```
+ CategoryInfo: NotSpecified: (:) [Start-DPMCloudRegistration], DlsException
```

```
+ FullyQualifiedErrorId :
```

```
CloudServiceRetryableError,Microsoft.Internal.EnterpriseStorage.Dls.UI.Cmdlet.CloudCmdlets.StartDPMCloudRegistration
```

NOTE: The corresponding log file is at the path C:\ProgramData\Microsoft Cloud Solutions\DeployDriver\BackupOnboarding.log on the Console VM.

These messages indicate that onboarding to Azure Backup failed. To work around this issue, you can manually onboard to Azure Backup. To manually onboard to Azure Backup, do the following:

- 1 On the Console VM, open Microsoft Azure PowerShell as an elevated user (Run as administrator), and then run the following commands, where *Prefix* is your stamp prefix (such as 557), and *VaultCredentialsFilePath* is a local folder on the console VM, for example c:\tempVCF\.

NOTE: If your environment uses a proxy server that requires credentials, first run the following command:

```
[System.Net.WebRequest]::DefaultWebProxy.Credentials = $ProxyCredential
```

```
Login-AzureRmAccount
```

```
$BackupVault = Get-AzureRMBackupVault -Name "<Prefix>BackupVault"
```

```
Get-AzureRMBackupVaultCredentials -Vault $BackupVault -TargetLocation
```

```
"<VaultCredentialsFilePath>"
```

- 2 In the Windows Azure Pack management portal for administrators, run the **Configure-BackuptoAzure** runbook. This runbook has the following parameters:

NOTE: For more information, see [How to run runbooks](#).

Table 16. Configure-BackuptoAzure runbook parameters

Parameter	Description
Passphrase	An alpha-numeric string of at least 16 characters that is used as an encryption key. IMPORTANT: You must store this key somewhere. You need it if you ever have to rebuild the DPM server.
ProxyCredential	Required only if proxy is enabled. You must specify a PowerShell Credential name.

Parameter

Description

NOTE: You must first create a PowerShell Credential asset in the management portal for administrators. In the portal, click **Automation > Assets > Add Setting > Add Credential**. Select **PowerShell Credential**, specify a name, and then enter a user name and password.

ProxyServerName	Required only if proxy is enabled. The FQDN of the proxy server.
ProxyServerPort	Required only if proxy is enabled. The proxy server port.
ReRegisterToAzure	Set to Yes.
VaultCredentialFilePathOnConsole	The local path on the Console VM to which you saved the vault credentials file, for example, <code>c:\tempVCF\BackupVault.VaultCredential</code> .

- 3 After you run the runbook, continue at step 7 of the previous procedure, [Onboard to Azure backup](#). You do not have to run the `BackupDeployDriver` script again.

Verify that DPM is attached to Azure

Do the following for verification:

- 1 Verify that DPM servers are attached to Azure.
 - a Open the DPM Central console or the DPM Administrator console and connect to a DPM server.
 - b Open the **Management** workspace.
 - c Click **Online** in the navigation pane, and verify that the **Azure Backup** registration was successful.

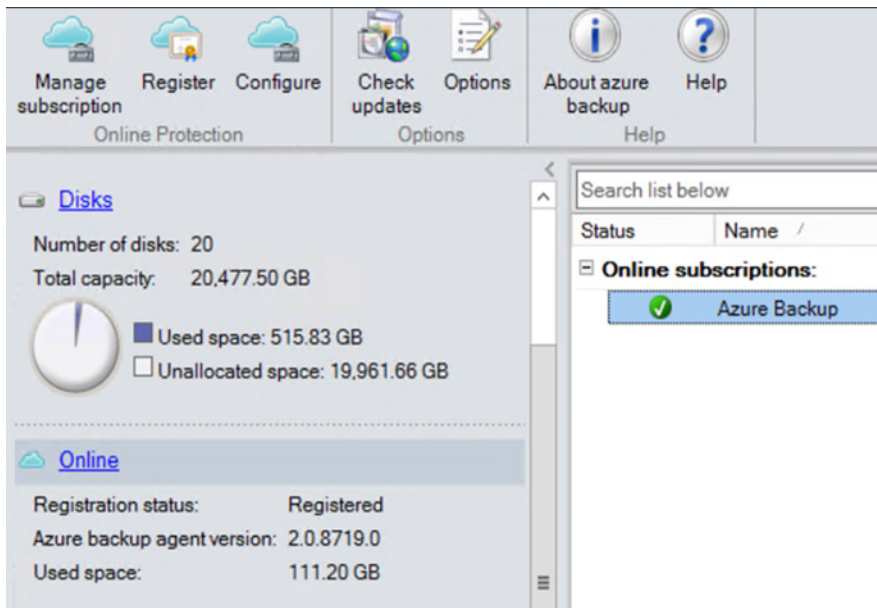


Figure 32. Azure Backup registration

- 2 Verify that infrastructure VMs and databases are protected to the cloud.
 - a Open the DPM Central console, or the DPM Administrator console, and connect to the DPM server that backs up the infrastructure components—typically, `<Prefix>DPM01`.
 - b Open the **Protection** workspace.
 - c In the **Online Protection** column, verify that the **Online Protection** column shows up as **Enabled**. (You may have to expand the tree to see this.)

Protection Group Member	Type	Protection Status	Online Protection
Protection Group: InfraVMGP (Total members: 7)			
Cluster Network Name: S20APA01.S20CCL.contoso.com			
\Online\S20APA01	Microsoft Hyper-V	OK	Enabled
Cluster Network Name: S20APT01.S20CCL.contoso.com			
\Online\S20APT01	Microsoft Hyper-V	OK	Enabled
Cluster Network Name: S20CON01.S20CCL.contoso.com			
\Online\S20CON01	Microsoft Hyper-V	OK	Enabled
Cluster Network Name: S20OM01.S20CCL.contoso.com			
\Online\S20OM01	Microsoft Hyper-V	OK	Enabled

Figure 33. Online Protection enabled

Default backup schedule and retention policy

By default, all infrastructure components are protected by DPM with the following schedule:

Table 17. Backup

Backup Policy for:	Target	Backup Frequency	Retention
Infrastructure VMs	Disk	Disk: Once per week; Saturday 8pm	Disk: 14 days
	Azure Backup—if opted in	Azure: Once per week; Sunday 8pm	Azure: 4 weeks
Infrastructure databases	Disk	Disk: Every 4 hours	Disk: 5 days
	Azure Backup—if opted in	Azure: Daily—10:00 PM	Azure: 10 days

NOTE: While these are the default settings, we recommend that you use the DPM Create Recovery Point Now option to back up a VM's databases before and after you make any configuration change.

By default, after you add a tenant VM to a protection group, tenant VMs are protected with the following schedule:

Table 18. Tenant VM backup schedule

Target	Backup Frequency	Retention
Disk	Daily—10:00 PM	7 days
Azure Backup—if opted in	Daily—6:00 AM	20 days

You can change the day of backup or time of day if you need to. If you change the schedule, make sure that you at least maintain the following backup frequency:

- For infrastructure VMs: Once a week backup with a two-week retention period
- For databases: Once every four hours backup with a five-day retention period

NOTE: Dell recommends that you do not change the number of recovery points because this impacts storage calculations.

DPM does not back up the DPM database. Instead, the DPM database is backed up through the Windows **DPMDBBackup** Task Scheduler job. The backup frequency is every 4 hours, and retention period is one day. The following table includes information about the DPM server database:

Table 19. DPM database

DPM Server Name	SQL Server Instance Name	Database Name
<Prefix>DMPO#	MSDPMDB	DPMDB_<Prefix>DPMO#

NOTE: DPM is used to back up the system databases in the MSDPMDB instance.

DPM protection groups

The following table provides information about the default protection groups for the infrastructure components:

Table 20. DPM protection groups

Protection Group	Data Sources
InfraDBPG	Instance level protection of all management infrastructure databases. These include databases for VMM, Operations Manager, SPF, Windows Azure Pack, SMA, and WSUS. Also protects the system databases on the DPM instance.
InfraVMPG	Protects all management infrastructure VMs.

When you protect tenant VMs, a protection group named **TenantVMs** is created.

Disable machine account password rotation on management VMs

Dell recommends that you disable machine account password rotation on all management VMs. If machine account password rotation is enabled, this can cause the recovery of management VMs to fail. If you recover a VM to a point in time that occurs before a machine account password reset occurred, logging on to the VM by using domain credentials fails with the error, "**The trust relationship between this workstation and the primary domain failed.**"

To avoid this failure, disable machine account password rotation on management VMs. To do this, a domain administrator can configure the **Domain Member: Maximum age for machine account** password Group Policy setting at the Dell Hybrid Cloud System for Microsoft OU level. For more information, see [Domain member: Disable machine account password changes](#) in Microsoft TechNet.

Protecting tenant VMs

An important feature of Dell Hybrid Cloud System for Microsoft is tenant VM protection. By default, tenant VMs are not protected. You must use a runbook to add them to a protection group in DPM.

Adding tenant VMs to backup

You must run the **Protect-TenantVMs** runbook to manage tenant VM protection

This runbook adds up to 75 newly created VMs to a protection group in DPM. You should run this runbook manually or through a scheduled task once each day. After a tenant VM is added to a protection group, by default:

- The tenant VM is configured for daily disk backup (10:00 PM), with a retention period of seven days.
- If cloud backup is enabled, the Azure backup starts at 6:00 AM daily with a retention period of 20 days.

The **Protect-TenantVMs** runbook is designed to protect 75 new VMs per run per day to ensure the following:

- That there is enough time for deduplication to complete deduplication of new data.
- That there is enough time to complete tenant VM backups.

Data deduplication runs on the local backup disks that are attached to the backup host. The data deduplication process reduces backup storage usage. There is a default schedule for data deduplication and for tenant backups. The default schedule is as follows:

- Deduplication: 6:00 AM to 10:00 PM
- Backup: 10:00 PM to 6:00 AM

You should plan to run the **Protect-TenantVMs** runbook so that it does not interfere with the backup window. Therefore, run it any time between 6:00 AM to 6:00 PM local time (at least three to four hours before the backup window starts).

If more than 75 new VMs were created, and you need to add them to a protection group on the same day, you can run the **Protect-TenantVMs** runbook more than once to protect the additional VMs. However, if you do so, DPM may not be able to complete the scheduled backups within the backup window, and deduplication may not be able to complete its run within its scheduled window. As a result, deduplication may not provide the predicted backup storage savings.

Excluding tenant VMs from backup

If you need to prevent protection of some tenant VMs to disk or to Azure, you can use the following runbooks to exclude or to restore protection.

Adding a VM to the exclusion list only works for unprotected VMs. If a VM is already protected, adding the VM name to the exclusion list does not stop protection of that VM. Therefore, you must exclude a VM from protection before you run the **Protect-TenantVMs** runbook.

Specify the VM names (wildcard characters are supported) or VMID (wildcard characters not supported) of the VMs for which you want to exclude or restore protection.

Table 21. Runbooks for exclusion

Backup Target	Runbook	Description
Disk	Add-DPMDiskExclusionItems	Use to prevent protection of specified tenant VMs to disk. When you exclude a VM from disk protection, it automatically means that there is no Azure protection for that VM.
Disk	Remove-DPMDiskExclusionItems	Use to restore protection of tenant VMs to disk. When you restore disk protection, it automatically enables Azure protection if the VM is not excluded from Azure protection through Add-DPMAzureExclusionItems .
Azure Backup	Add-DPMAzureExclusionItems	Use to prevent protection of specified tenant VMs to Azure. If disk protection is enabled for the VM, that protection continues.
Azure Backup	Remove-DPMAzureExclusionItems	Use to restore protection of tenant VMs to Azure.

Validate that the tenant VMs are protected

After you run the **Protect-TenantVMs** runbook, you can view which DPM server will protect the tenant VM by using the VMM console.

- 1 In the VMM console, open the **VMs and Services** workspace.
- 2 On the **Home** tab of the ribbon, in the **Show** group, click **VMs**.
- 3 In the **VMs** list, locate the VM, and then view the information in the **ProtectedByDPMServer** column.

Modifying tenant protection policies

If you want to change the default values for tenant VM protection, you can use the **Modify-DPMTenantProtectionConfiguration** runbook.

The following table lists the parameters and their default values:

Table 22. Runbook parameters

Parameter Name	Description	Required/Optional
AzureBackupStartTime	The Azure backup start time. Make sure this starts after the disk backup window is over. By default, this is 6:00 AM.	Optional
AzureRetentionRange	Retention range, in days, for Azure. By default, this is 20 days.	Optional
BackupWindowDuration	The backup window duration. By default, this is 8 hours	Optional
BackupWindowStartTime	The tenant disk backup start time. By default, this is 10:00 PM.	Optional
CCWindowDuration	The consistency check window duration. Keep this as backup duration plus 1 hour at the minimum. By default, this is 9 hours.	Optional
CCWindowStartTime	The consistency check window start time. Keep this 1 hour before the backup window start time.	Optional
RetentionRange	The disk retention period for tenant backups, in days. By default, disk retention is 7 days.	Optional

Recovering VMs and databases—high level

This section includes the general steps for VM and database recovery for management components.

NOTE: These are high-level procedures. When you recover a component, refer to the component's specific recovery steps as described in the [Recovering from management component failures](#) and [Recovering a tenant VM](#) sections. These sections provide important pre- and post-recovery steps, and guidance around which recovery method to use.

Recovering a VM to its original location

Do the following:

- 1 Open the DPM Administrator console, and click **Recovery**.
- 2 In the navigation tree, expand the VM that you want to recover.
- 3 Under the VM, click **All Protected HyperV Data**.

- 4 In the **Recovery points** pane do the following:
 - a Under **Recoverable Item**, click the VM that you want to recover.

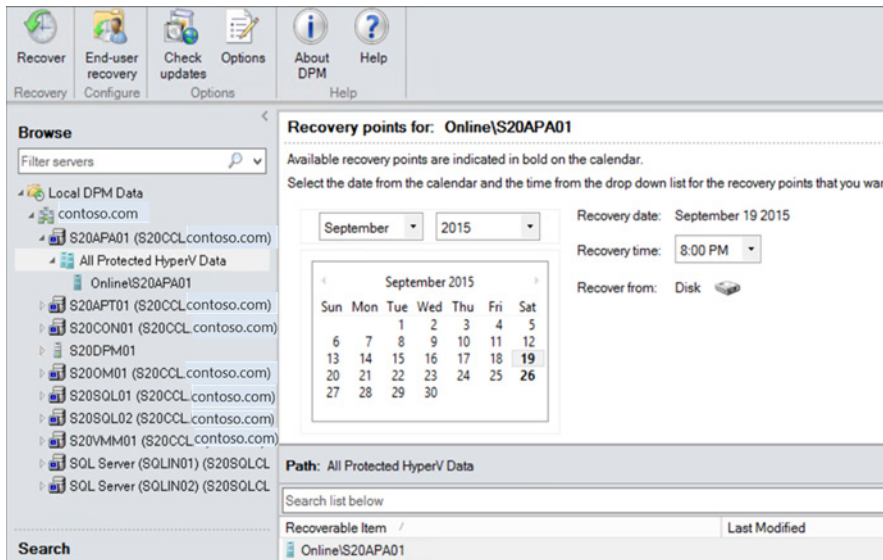


Figure 34. Recoverable item

- b Click any date and time in the calendar to see available recovery points. Dates that show as **bold** have active recovery points. To minimize data loss, it is important to choose to recover from the latest possible recovery point.
 - c To select the recovery source, in the **Recovery time** list, select a recovery point that either indicates **Disk** or **Online** (from Azure).
 - d On the ribbon, click **Recover** to start the Recovery Wizard.
- 5 In the Recovery Wizard, in the **Select recovery type** page, select **Recover to original instance**.
- 6 On the **Specify Recovery Options** page, leave the **Network bandwidth usage throttling** and **SAN Recovery** selections without any modifications.
- 7 On the **Summary** page, review your settings, and then click **Recover**.
- 8 After the recovery finishes, click **Close** to close the Recovery Wizard.
- 9 Start the VM that you just recovered.
- 10 After you recover the VM, you must synchronize it as follows. The **Protection Status** of this VM shows as **Replica Inconsistent** until it is synchronized.
 - a In the DPM Administrator Console, open the **Protection** workspace.
 - b Locate and then right-click the recovered VM. Click **Perform consistency check**.
 - c In the **Microsoft System Center 2012 R2 Data Protection Manager** dialog box, click **Yes** to perform the consistency check.

Recovering a VM to an alternate location

You can use this procedure to recover a tenant VM to an alternate location. Do this procedure if a tenant VM was deleted from VMM or from the Windows Azure Pack management portal for tenants.

IMPORTANT: Before you perform this procedure, make sure that you review the [Recovering a tenant VM](#) section.

- 1 Follow the first four steps described previously in [Recovering a VM to its original location](#).
- 2 On the **Select Recovery Type** page, click **Copy to a network folder**.

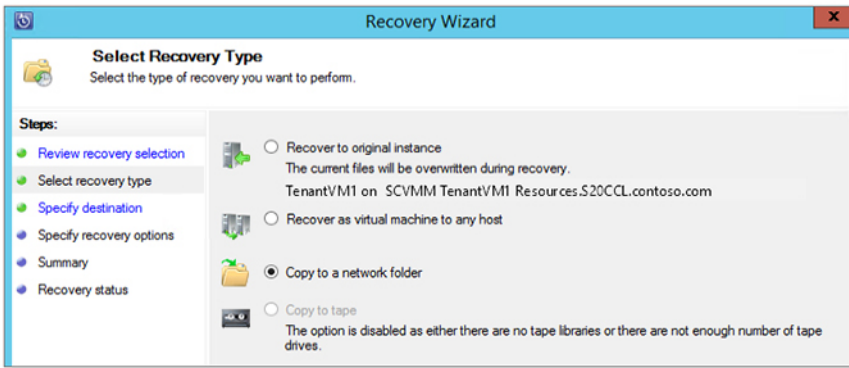


Figure 35. Select Recovery Type

- 3 On the **Specify Destination** page, click **Browse**. Locate one of the Scale-Out File Server nodes, and then expand **Volumes > C:\ > ClusterStorage**.
- 4 Select any clustered volume that is mapped to a production share. Although not required, as a best practice, create a folder in the share on the SOFS that you can point to, such as a **VM Recovery** folder. The following graphic illustrates this folder:

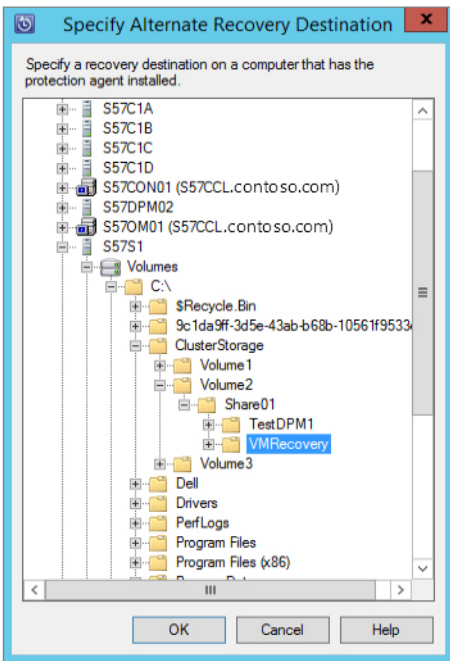


Figure 36. Alternate recovery folder

- 5 Complete the wizard using the default options to recover the VM files.
- 6 Next, create a VM from the Windows Azure Pack management portal for tenants with the same name of the VM that you want to recover.
- 7 In the VMM console, shut down the new VM.
- 8 Next, you must remove the VHDs of the newly created VM, and add the VHDs that you recovered in the production share earlier in this procedure.
 - a Get the VM location by running the following command:


```
Get-SCVirtualMachine-Name <VMName> | select Location
```
 - b In the VMM console, in the **VMs and Services** workspace, right-click the VM, click **Properties**, and then click the **Hardware Configuration** tab.
 - c Remove all the current VHDs.

- d Copy all the VHDs that you recovered earlier to the location you obtained in step 8a.
 - e If there are differencing disk VHDs, copy the VHDs with the correct folder hierarchy.
 For example, there is a child VHD at the following path: \\s20sfs.contoso.com\Share01\asd\DPM_9-15-2015_8.39.7\Recovered_At_9-15-2015_10.1.25\s20sfs-Share01-Vol\NewVM1\child.vhdx
 There is a parent VHD at the following path: \\s20sfs.contoso.com\Share01\asd\DPM_9-15-2015_8.39.7\Recovered_At_9-15-2015_10.1.25\s20sfs-Share01-Vol\Parent1.vhdx
 Compare the paths, and look for where the path is not the same—bold in the examples. Copy the uncommon content to the location that you obtained in step 8a. In this example, you would copy the **NewVM1** folder, and its contents, and **Parent1.vhdx**.
 - f If there is no differencing disk VHD, add all the VHDs to the VM. If there is a differencing disk VHD, add only the child VHD.
- 9 Start the VM.
 You do not have to perform a consistency check because this VM is a new VM. It will be protected separately by DPM during the next run of the **Protect-TenantVMs** runbook. The old VM recovery points are deleted automatically after they reach retention range limits.

Recovering a database to its original location

As part of a recovery process, recovering management component databases by using DPM is an important step. The following procedure provides the general steps for database recovery.

NOTE: When you recover a specific component, you must follow the component's specific recovery steps as described in [Recovering from management component failures](#).

- 1 In the DPM Administrator console, open the **Recovery** workspace.
- 2 Expand **SQL Server** (for the instance of SQL Server that hosts the database that you want to recover), expand **All Protected SQL Instances**, and then expand the instance.
- 3 Select the database that you want to recover, for example:

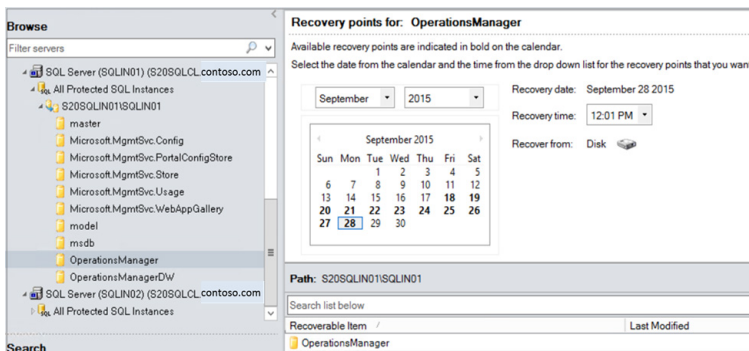


Figure 37. Select database

- 4 In the **Recovery points** pane, select a recovery point:
 - a Click any date and time in the calendar to see available recovery points. Dates that are shown in **bold** have active recovery points. To minimize data loss, it is important to choose to recover from the latest possible recovery point
 - b To select the recovery source, in the **Recovery time** list, select a recovery point that either indicates **Disk** or **Online** —from Azure.
 - c On the ribbon, click **Recover** to start the Recovery Wizard.
- 5 In the Recovery Wizard, on the **Select Recovery Type** page, select **Recover to the original instance of SQL Server (Overwrite database)**, and then click **Next**.
- 6 If doing a disk restore, on the **Specify Database State** page, keep the default setting of **Leave database operational**.
- 7 On the **Specify Recovery Options** page, leave the **Network bandwidth usage throttling** and **SAN Recovery** settings without any changes.
- 8 On the **Summary** page, review your settings and then click **Recover**.
- 9 After the recovery finishes, click **Close** to close the Recovery Wizard.

- 10 After you recover a database, it must be synchronized by DPM. The **Protection Status** of this database is **Replica Inconsistent** until you synchronize it as follows:
 - a In the DPM Administrator console, open the **Protection** workspace.
 - b Right-click the recovered database, and then click **Perform consistency check**.
 - c In the **Microsoft System Center 2012 R2 Data Protection Manager** dialog box click **Yes** to perform the consistency check.

Recovering a datasource to an alternate DPM server

If a DPM server is unavailable and cannot be recovered, you can recover datasources, such as VMs or databases, that were protected by that DPM server to a working DPM server from Azure Backup.

- 1 In the Azure portal, click **Recovery Services**, and then click the backup vault.
- 2 Click **Download vault credentials**, and download your vault credentials to a location on the Console VM.

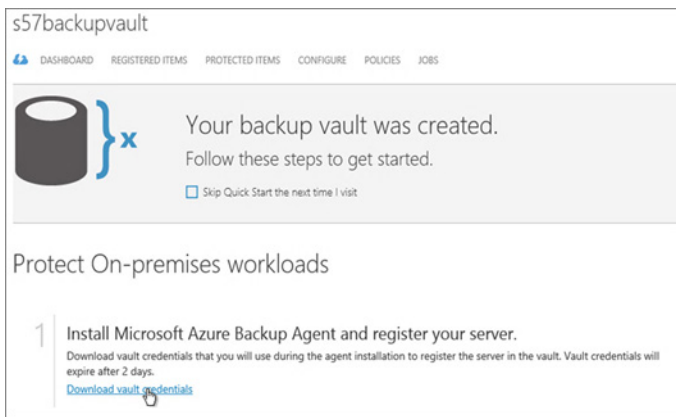


Figure 38. Download vault credentials

- 3 In the DPM Administrator console, in the **Recovery** workspace, click **Add External DPM** on the ribbon.

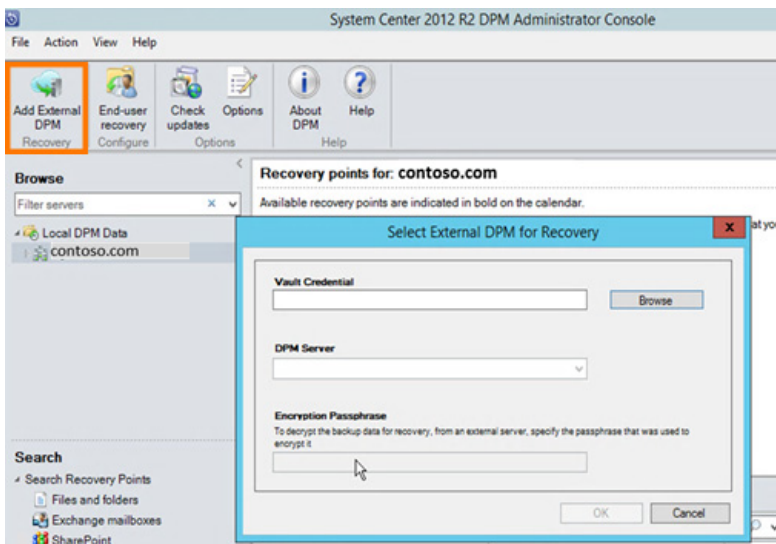


Figure 39. Add External DPM

- 4 Click **Browse**, and then select vault credentials file that you downloaded. This step populates the list of registered servers in the **DPM Server** list.
- 5 Select the server that you want, enter the encryption passphrase, and then click **OK**. A job to get the datasources starts. You can monitor the job on the **Monitoring** tab.

- 6 When the job finishes, you can browse the protected online datasources. Select a datasource to see the available online recovery point.
- 7 Select a recovery point, and follow the usual recovery steps.
- 8 To return to the local DPM data view, click **Clear external DPM**.

Recovering from management component failures

This section describes how to recover from data failures of various management components in the Dell Hybrid Cloud System for Microsoft environment.

This section lists the steps that are specific to database recovery, and the steps that are specific to VM recovery. Follow the respective steps for each component, for database or VM recovery, as needed.

NOTE: Perform all procedures in this section by using an account that is a member of the *<Prefix>-Ops-Admins* group.

Recovering Operations Manager

A key Operations Manager role is monitoring the entire Dell Hybrid Cloud System environment.

If you have exhausted all options when trying to recover from Operations Manager failures, you can recover Operations Manager data to restore functionality.

Recovering the Operations Manager database

- 1 From the VMM console, shut down the Operations Manager VM—*<Prefix>OM01*.
- 2 Use the steps in [To recover a database to its original location](#) to recover the following Operations Manager databases. To minimize data loss, select the latest recovery point.

Table 23. Operations Manager Databases

SQL Server Instance	Database Name
SQLIN01	Operations Manager
	Operations Manager DW

- 3 For the SQL Server instance, enable Service Broker by doing the following:
 - a On the Console VM, open SQL Server Management Studio.
 - b Connect to the SQL Server cluster and instance.

Table 24. SQL Server Cluster

SQL Server Cluster Name	SQL Server Instance
<i><Prefix></i> SQLCL	SQLIN01

- c Connected to the instance that is specified in the table, run the following T-SQL commands:


```
ALTER DATABASE OperationsManager SET ENABLE_BROKER
```

```
ALTER DATABASE OperationsManagerDW SET ENABLE_BROKER
```
- 4 Start the Operations Manager VM.
- 5 Detect and repair any data consistency issues by following the steps in [How to use data consistency runbooks](#).

Recovering the Operations Manager VM

- 1 From the VMM console, shut down the Operations Manager VM (*<Prefix>OM01*).
- 2 Use the steps described in [Recovering a VM to its original location](#) to recover the Operations Manager VM. To minimize the data loss, select the latest recovery point.

- 3 Restart the Operations Manager VM.
- 4 Detect and repair any data consistency issues by following the required steps in [How to use data consistency runbooks](#).

Recovering VMM

VMM plays a key role in managing the hosts and VMs in the Dell Hybrid Cloud System for Microsoft environment.

If you have exhausted all options trying to recover from application failure, you can use DPM to recover the VMM database to a previous point in time. You can:

- Recover the VMM database
- Recover the VMM VM, and
- Verify that the VMM library server is working.

Recovering the VMM database

- 1 From the Console VM, open Failover Cluster Manager.
- 2 Connect to the compute cluster.
- 3 Shut down the VMM VM (**<Prefix>VMM01**).
- 4 Use the steps in [Recovering a database to its original location](#) to recover the following VMM database. To minimize data loss, select the latest recovery point.

Table 25. VMM Database Name

SQL Server Instance	Database Name
SQLIN02	VirtualManagerDB

- 5 Open Failover Cluster Manager, and connect to the compute cluster.
- 6 Start the VMM VM.
- 7 In the VMM console, verify that the content in the **Fabric** workspace is updated.
- 8 Detect and repair any data consistency issues by following the required steps in [How to use data consistency runbooks](#).

Recovering the VMM VM

- 1 From the Console VM, open Failover Cluster Manager.
- 2 Connect to the compute cluster.
- 3 Shut down the VMM VM (**<Prefix>VMM01**) that is located on the compute cluster.
- 4 Use the steps in [Recovering a VM to its original location](#) to recover the VMM VM. To minimize data loss, select the latest recovery point.
- 5 In Failover Cluster Manager, connect to the compute cluster, and then click **Roles**. In the **Roles** pane, right-click the VMM VM, and then click **Start**.
- 6 Detect and repair any data consistency issues by following the required steps in [How to use data consistency runbooks](#).

Verifying the VMM library server is working

If you recovered the VMM VM, you should verify that the VMM library is working correctly.

- 1 After recovery, open the VMM console, and then open the Library workspace.
- 2 Under **Library Servers**, verify that the VMM server is listed as the library server, with the correct library shares of **MSSCVMLibrary**.
- 3 If the library server or share does not appear, see the TechNet Library article [How to Add a VMM Library Server or VMM Library Share](http://technet.microsoft.com/library/gg610579.aspx) (<http://technet.microsoft.com/library/gg610579.aspx>). You can use the existing **<Prefix>-System Run As** account to add the library server.
- 4 Right-click the library server, and then click **Refresh**.

Recovering SMA

SMA reduces an administrator's burden by providing the ability to automate many manual tasks. If all options for recovery from application failures are exhausted, you can recover SMA data to restore functionality.

Recovering the SMA database

- 1 From the VMM console, shut down the VM that is hosting SMA (<Prefix>APA01).
- 2 Use the steps in [Recovering a database to its original location](#) to recover the following SMA database. To minimize data loss, select the latest recovery point.

Table 26. SMA Database Name

SQL Server Instance	Database Name
SQLIN02	SMA

- 3 From the VMM console, restart the APA01 VM.
- 4 Detect and repair any data consistency issues by following the required steps in [How to use data consistency runbooks](#).

Recovering the APA VM—with SMA, SPF

- 1 In the VMM console, in the VMs and Services workspace, use the **Connect via Console** option to log on to the <Prefix>APA01 VM.
- 2 Stop the Runbook service—**rbsvc**. To do this, start a Windows PowerShell session, and then run the following command:
Stop-Service rbsvc

The service can take up to 20 minutes to stop. Wait for the service to stop before you continue to the next step.

- 3 From the VMM console, shut down the VM.
- 4 Use the steps in [Recovering a VM to its original location](#) to recover the VM. To minimize data loss, select the latest recovery point.
- 5 From the VMM console, start the VM.
The Runbook service starts automatically.
- 6 Detect and repair any data consistency issues by following the steps in [How to use data consistency runbooks](#).

Recovering SPF

If all options of recovering from SPF failures are exhausted, you can use DPM to recover SPF data to restore SPF functionality. To recover the SPF database:

- 1 From the VMM console, shut down the VM that is hosting SPF (<Prefix>APA01).
- 2 Use the steps in [Recovering a database to its original location](#) to recover the following SPF database.

Table 27. SPF Database Name

SQL Server Instance	Database Name
SQLIN02	SCSPFDB

- 3 From the VMM console, start the VM.
- 4 Detect and repair any data consistency issues by following the required steps in [How to use data consistency runbooks](#).

Recovering Windows Azure Pack

Windows Azure Pack provides the portals (and additional features) where application administrators and subscribers manage their resources. If all options to recover from Windows Azure Pack failures are exhausted, you can recover the Windows Azure Pack databases and VMs by using DPM.

Recovering Windows Azure Pack databases

- 1 If any of the Windows Azure Pack databases fail, you must recover the database to a previous time stamp. Then, run the data consistency runbooks to determine the next steps that you must take. From the Console VM, open the VMM console.
 - a Shut down the Windows Azure Pack tenant portal VM.
 - b Shut down the Windows Azure Pack admin portal VM.
- 2 Use the steps in [Recovering a database to its original location](#) to recover the following Windows Azure Pack databases. To minimize data loss, select the latest recovery point.

Table 28. Windows Azure Pack Databases

SQL Server Instance	Database Name
SQLIN01	<ul style="list-style-type: none">• Microsoft.MgmtSvc.Config• Microsoft.MgmtSvc.PortalConfigStore• Microsoft.MgmtSvc.Store• Microsoft.MgmtSvc.Usage• Microsoft.MgmtSvc.WebAppGallery

- 3 Detect and repair any data consistency issues by following the required steps in [How to use data consistency runbooks](#).
- 4 From the VMM console, do the following:
 - a Start the Windows Azure Pack admin VM—**<Prefix>APA01**.
 - b Start the Windows Azure Pack tenant VM—**<Prefix>APT01**.

Recovering Windows Azure Pack VMs

- 1 From the VMM console, do the following:
 - a Shut down the Windows Azure Pack tenant VM (**<Prefix>APT01**).
 - b Shut down the Windows Azure Pack admin VM (**<Prefix>APA01**).
- 2 Use the steps in [Recovering a VM to its original location](#) to recover all the VMs that you shut down in step 1.
- 3 From the VMM console, do the following:
 - a Start the Windows Azure Pack admin VM (**<Prefix>APA01**).
 - b Start the Windows Azure Pack tenant VM (**<Prefix>APT01**).
- 4 Detect and repair any data consistency issues by following the required steps in the [How to use data consistency runbooks](#) section.

SQL Server VM recovery

To recover a SQL Server VM:

- 1 Log on to the Console VM.
- 2 Start Failover Cluster Manager, and then connect to the SQL Server cluster **<Prefix>SQLCL**.
- 3 Evict the node that you want to recover, for example **<Prefix>SQL02**. To do this, under the cluster name, click **Nodes**. Right-click the node that you want to evict, point to **More Actions**, and then click **Evict**.
- 4 Under **Nodes**, verify that the server you evicted is no longer listed.
- 5 Use the steps in [Recovering a VM to its original location](#) to recover the SQL Server VM.
- 6 From the VMM console, start the SQL Server VM.

- 7 Validate that all nodes in the SQL Server cluster (<Prefix>SQL01 and SQL02) are up and running.
- 8 If the node is not attached to the cluster, then add the node to the SQL Server cluster.
- 9 Detect and repair any data consistency issues by following the required steps in [How to use data consistency runbooks](#).

Recovering a tenant VM

By default, all tenant VMs that are deployed as VM roles are deployed with a single parent VHD, and therefore use a differencing disk. DPM's original location recovery work flow (described in [Recovering a VM to its original location](#)) will not work for tenant VMs that use a differencing disk.

NOTE: You must perform the procedures in this section as a member of the <Prefix>-Diag-Admins group.

Determine whether the VM uses a differencing disk

To recover a tenant VM, you must first check whether the VM has a shared parent VHD configuration.

- 1 On a Console VM, open Windows PowerShell ISE.
- 2 Run the following script. Update the value of `VM_Name` with the name of the VM that you want to recover.

```
vmname = "VM_Name"

$VHDMap = @{}

$VmsWithParentVHDs = @{}

$vmns = Get-SCVirtualMachine

foreach($VM in $vmns)
{
    foreach($vhd in $vm.VirtualHardDisks)
    {
        if($vhd.ParentDisk -ne $null)
        {
            if($VHDMap[$vhd.ParentDisk.ID] -ne $null)
            {
                $VHDMap[$vhd.ParentDisk.ID] += "," + $vm.Name

                $dummyVms = $VHDMap[$vhd.ParentDisk.ID].split(",");
                foreach($dummyVm in $dummyVms)
                {
                    if($VmsWithParentVHDs[$dummyVm] -eq $null)
                    {
                        $VmsWithParentVHDs.Add($dummyVm, "1")
                    }
                }
            }
        }
    }
}
```

```

        }
    else
    {
        $VHDMAP.Add($vhd.ParentDisk.ID , $vm.Name)
    }
}

}

if($VmsWithParentVHDs[$vmname])
{
    Write-Host "The VM has a parent VHD configuration."
}
else
{
    Write-Host "The VM does not have a parent VHD configuration."
}

```

The script output indicates whether the VM has a parent VHD configuration.

Recovering a VM with no parent VHD configuration

To recover a VM with no parent VHD configuration, that is, a VM that uses a differencing disk, do the following.

- 1 **Case 1, the VM is corrupted but not deleted:**
 - a In the VMM console, shut down the VM that you want to recover.
 - b Use the steps in [Recovering a VM to its original location](#) to recover the VM.
 - c From the VMM console, start the VM.
- 2 **Case 2, the VM is deleted:**
 - a Use the steps in [Recovering a VM to an alternate location](#) to recover the VM.
 - b From the VMM console, start the VM.

Recovering a VM with a parent VHD configuration

To recover a VM with a parent VHD configuration, that is, it uses a differencing disk, do the following:

- 1 If the VM is present in the Windows Azure Pack management portal for tenants, delete the VM from the portal.
- 2 Use the steps in [Recovering a VM to an alternate location](#) to recover the VM.
- 3 From the VMM console, start the VM.

Recover a tenant VM from Azure with a size bigger than staging area

During recovery from Azure Backup, backup data from Azure Backup must be temporarily downloaded to a local staging area before it is recovered to the final recovery destination.

By default, the staging area is located on the DPM server, at the path **E:\StagingArea**. By default, the **E:** volume is 2 TB in size. If the VM that you want to recover is too large for the staging area, you must modify the staging area to point to a larger storage location.

The following procedure shows how to create a VHD on a remote server, and expose it as an iSCSI disk in the DPM server. You can perform similar steps if you have a storage array network (SAN), or any other storage that can be exposed as an iSCSI target.

Step 1 Create the iSCSI target disk on a server with available storage

On a Windows Server 2012 R2 server that has large available storage, create the iSCSI target disk.

- 1 Open a Windows PowerShell session, and run the following commands:

```
Add-WindowsFeature FS-iSCSITarget-Server
```

```
Add-WindowsFeature iSCSITarget-VSS-VDS
```

- 2 Create the iSCSI target disk.

- a Open Server Manager, and click **File and Storage Services**.
- b Click **iSCSI**.
- c In the **iSCSI Virtual Disks** pane, right-click, and then click **New iSCSIVirtual Disk**. Follow the wizard to create the iSCSI target.
- d On the **Access Servers** page, when you add the access server, in the **Type** list, click **IP Address**, and specify the IP address of the target DPM server on which you want to do recovery. To obtain the IP address, run the command:

```
ping <DPM server name> -4
```

For example:

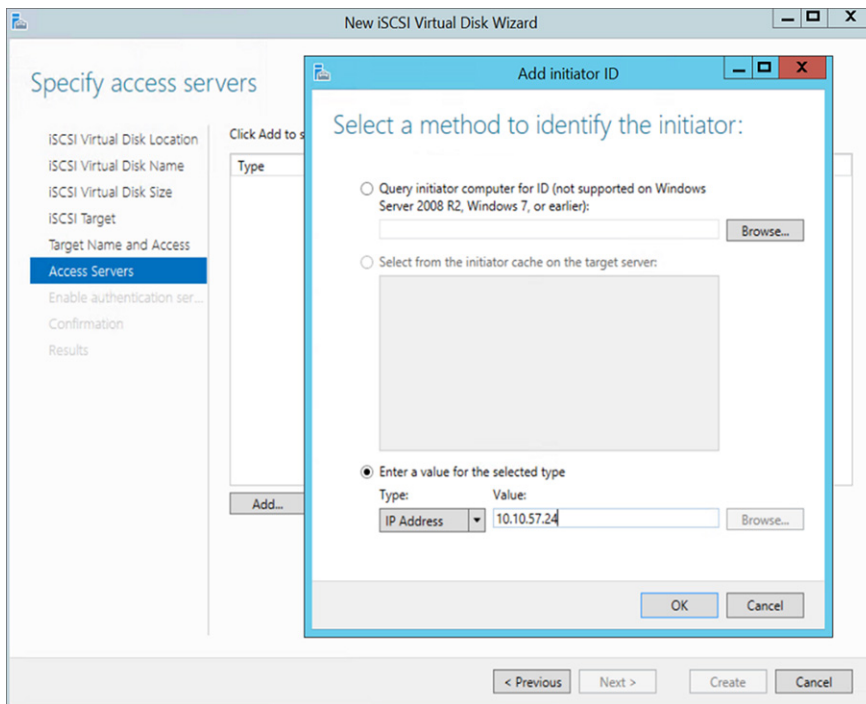


Figure 40. Add initiator ID

- 3 Click **Next**, and follow the wizard to complete the VHD setup.

Step 2 Add the iSCSI disk to the DPM server as a staging area

- 1 Log on to the DPM server and start the iSCSI initiator. In Server Manager, on the **Tools** menu, click **iSCSI Initiator**. When prompted to start the service, click **Yes**.

The **iSCSI Initiator Properties** dialog box opens.

- 2 In the **Target** box, enter the name or IP address of the source server (that is, the server on which you created the iSCSI disk), click **Quick Connect**, and then click **Done**.

The target should show as **Connected**.

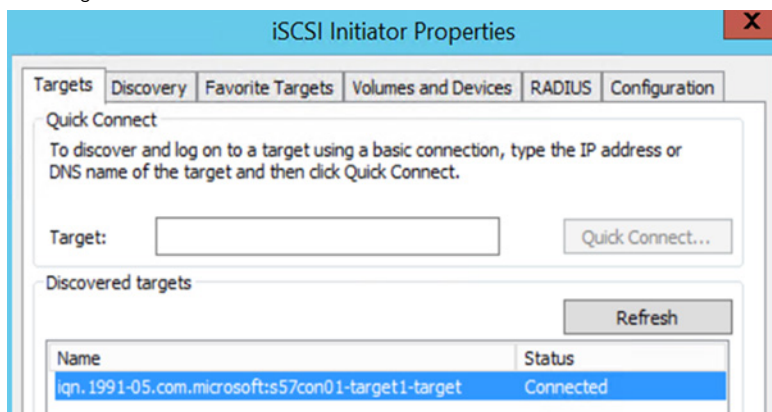


Figure 41. Target connected

- 3 Open Disk Management, initialize the newly added disk, and create a volume.
- 4 Change the staging area to point to this disk.
 - a In the DPM Administrator console, open the **Management** workspace.

- b Click **Online**.
- c On the ribbon, in the **Online Protection** group, click **Configure**.

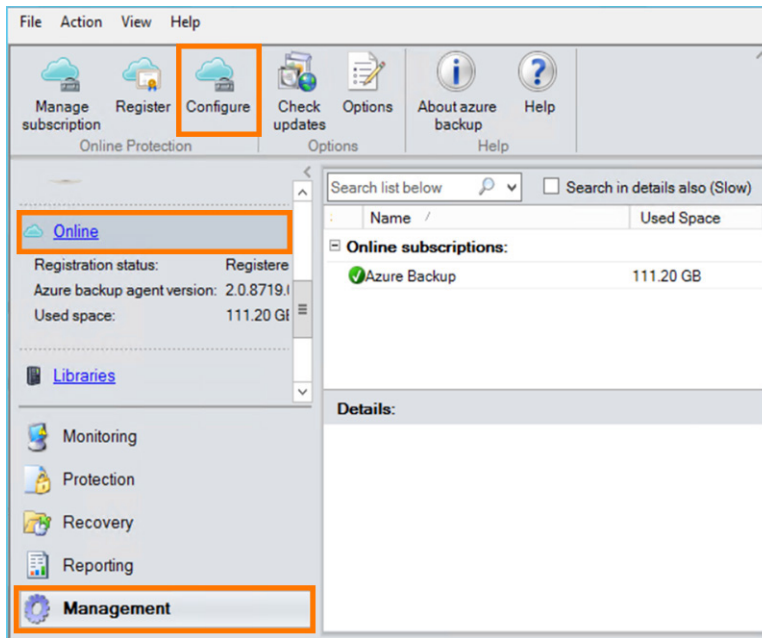


Figure 42. Configure Online Protection

- d On the **Recovery Folder Settings** page, point to the new volume (or folder on that volume) that you added.

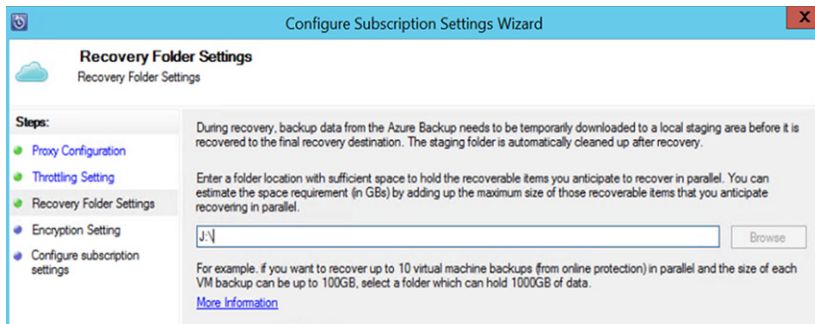


Figure 43. Recovery Folder Settings

- 5 Now recover the VM.
- 6 After you recover the VM, clean up the configuration.
 - a Reconfigure the DPM staging area to point to the original location (**E:\StagingArea**).
 - b Remove the iSCSI connection by disconnecting it via the iSCSI initiator.
 - c Delete the VHD from the source server.

Recovering DPM from DPM failures

You can use DPM to back up and recover management infrastructure components. If DPM itself fails, you cannot recover from subsequent component failures. This section describes some of the DPM failure scenarios and the steps that are needed to recover from DPM server failures.

Determining whether to recover or rebuild

If you have trouble with a DPM server, you can either perform DPM recovery or you can rebuild the DPM server. Use the following steps to determine which method to choose.

- 1 Log on to the backup host (or browse through a network connection), and do the following:
 - a Browse to `H:\<DPMVMName>\Virtual Hard Disks`.
 - b For each DPM VM, verify that there is a `<Prefix>DPM0#-Scratch` VHD file listed.
- 2 On the Console VM, in the VMM console, check the DPM VM properties.
 - a In the **VMs and Services** workspace, right-click the DPM VM, click **Properties**, and then click the **Hardware Configuration** tab.
 - b Under **Bus Configuration**, click each disk to see the locations of the backup VHDs. In the path of the VHDs, look for names in the format `<DPMName>Backup#.vhd`. There should be 20 (unless you added more).
- 3 If all VHDs exist, try to recover DPM.
- 4 If the disks are not intact, or you tried recovery and it was unsuccessful, rebuild the DPM server.

Recovering a DPM server

If you determine recovery of the DPM server is required, do the following:

- 1 Remove the host from VMM.
 - a In the VMM console, open the **VMs and Services** workspace.
 - b Under the **All Hosts** host group, remove the backup host on which the DPM VM resides.
- 2 Remove the corrupted DPM VM from Operations Manager.
 - a Open the Operations Console.
 - b In the **Administration** workspace, expand **Device Management > Agent Managed**.
 - c Right-click the corrupted DPM server, and then click **Delete**.
- 3 On the Console VM, open Hyper-V Manager and connect to the backup host.
- 4 Delete the corrupted DPM VM.
- 5 Log on to the backup host on which the DPM server resides.
- 6 From a command prompt, change directories to `D:\<DPMName>\Virtual Hard Disks`, and delete all the VHDs in this folder.
- 7 At a command prompt, run the following commands to enable the default local Administrator account, and to make sure the password is set correctly. For this procedure, this account must have a specific password assigned:

```
net user administrator /active:yes
net user administrator pass2015@MSPCS
```
- 8 Log off, and then back on to the Console VM as the default local Administrator account with the password `pass2015@MSPCS`.
- 9 Update the manifest .XML file for redeployment.
 - a Open the .XML file at `C:\Program Files\Microsoft Cloud Solutions\DeployDriver\Manifests\DeploymentManifest.xml`.
 - b Update the backup host configuration. Search for the backup host name in the .xml file, locate the name of the backup host (for example, S20B01) in the `<BackupConfiguration>` section of the file, and change the `DeploymentStatus` to "DomainJoined". For example:

```
<BackupConfiguration>

<Nodes>

<Node Name="S20B01" DeploymentStatus="DomainJoined" ConfigurationID="828bc360-fd65-4304-
bc50-81ea4027ad7f" Password="" SerialNumber="22PGD42">
```
 - c Update the DPM node configuration. Search for `<BackupVMs>` in the file. For each DPM server, update `DeploymentStatus` to "DomainJoined". For example:

```
<BackupVMs>
```

```

<Role Type="DPM" DeploymentStatus=" DomainJoined" Name="S20DPM01" BackupHostName="S20B01"
ConfigurationID="02651dd9-3028-45a8-9188-9997aa816418" Password="">

<IPv4Addresses>

<IPv4Address NetworkId="Management">10.10.20.32</IPv4Address>

</IPv4Addresses>

<BackupVhd NumberOfVHDs="20" VhdSize="1024" />

</Role>

<Role Type="DPM" DeploymentStatus="DomainJoined" Name="S20DPM02" BackupHostName="S20B01"
ConfigurationID="b7a1b6bd-23ff-4f4b-b68e-20ac5e19d005" Password="">

```

d If you are running version 1.1 or later, do the following:

- 1 In the <BackupVMs> section, if the following line exists, remove it for each DPM VM:

```

<BackupVhd NumberOfVHDs="20" VhdSize="1024" />

```
- 2 Search for the <BackupDisk> section. Note the size values for XXXX and YYYY, and then replace the following:

```

<BackupDisk>
  <Volumes>
    <Volume Type="Scratch" Size="XXXX" />
    <Volume Type="Backup" Size="YYYY" />
    <Volume Type="Backup" Size="YYYY" />
    <Volume Type="Backup" Size="YYYY" />
  </Volumes>
</BackupDisk>

```

With this—updating with the same values for XXXX and YYYY that were used previously:

```

<BackupDisk>
  <Volumes>
    <Volume Type="Scratch" Size="XXXX" />
    <Volume Type="Backup" Size="YYYY" NumberOfVolumesPerDPM="3" />
  </Volumes>
  <BackupVhd NumberOfVHDsPerDPM="20" VhdSize="1024" />
</BackupDisk>

```

10 Set the password field in the .xml file for the backup host.

- a In a Windows PowerShell session, run the following script to set the \$password variable to the password you want to set.

```

password = "YourPassword"
ConvertTo-SecureString $password -AsPlainText -Force |

ConvertFrom-SecureString

```

- b Copy the output of this script.
- c In the .XML file, search for the backup host name, and paste the output from the previous step between the quotes in the Password="" field.

```

<BackupConfiguration>

<Nodes>

<Node Name="S20B01" DeploymentStatus="DomainJoined" ConfigurationID="828bc360-fd65-4304-
bc50-81ea4027ad7f" Password="PasswordOutput" SerialNumber="22PGD42">

```

For example:

```

<BackupConfiguration>
<Nodes>

```

```
<Node Name="S20B01" DeploymentStatus="DomainJoined" ConfigurationID="828bc360-fd65-4304-
bc50-81ea4027ad7f"
Password="01000000d08c9ddf0115d1118c7a00c04fc297eb0100000012adbc74a67cfe48ac4404f29b4d43c
c0000000020000000001066000000010000200000001565d7d65f0ca2fcf0e0d82f24c481689ccdb7aa4d85
ac400906c7768e6228ba00000000e8000000002000020000000750649ad99b3809f7b66f9eb1ff4bb67afa10
8bac79372a56b53ca81ef235c5e30000000eb537f00952fc2d36d3821571b65fc7ccca26066e47eb5de0be691
9a3a24f08e693031d3b8928e1cfa00d32410dfacda40000000e53617e63be31270a1ed37cb2f54682f802a171
41153741f454be9b3ec7fc6fff1cc0e1a3ca2e56fb7f7af16c5d4a6fd71e0d91c742b38782e03a648c8eb39da
" SerialNumber="22PGD42">
```

- d On the backup host, open a Windows PowerShell session as an elevated user, and then run the following commands to enable the local administrator account, and to update to the same password that you specified for `$password`, in step 10a (that is, the plain text password):

```
net user administrator /active:yes
```

```
net user administrator <password>
```

- 11 Set the password field in the .xml file for the DPMs VMs.

- a In a Windows PowerShell session, run the following script to set the `$password` variable to the password you want to set.

```
$password = "YourPassword"
```

```
ConvertTo-SecureString $password -AsPlainText -Force |
ConvertFrom-SecureString
```

NOTE: If you want to use the same password as the backup host, you can skip this step and in step 10c, copy the same encrypted password string.

- b Copy the output of this script.
- c Using the output of this script, search for node `<BackupVMs>` in the .xml file, and update the `Password=""` field for all the DPM VMs on that backup host.
- d On the DPM that is not corrupted, run the following commands to enable the local administrator and to update the password. Specify the same password that you used for `$password` in step 11a (that is, the plain text password).

```
net user administrator /active:yes
```

```
net user administrator <password>
```

- 12 On the Console VM, update the registry subkey for deployment status.

- a Open Registry Editor.
- b Locate the following registry subkey: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cloud Solutions\Deployment\Status**
- c Update the values for the backup host and the DPM VMs from **Deployed** to **DomainJoined**. For example:

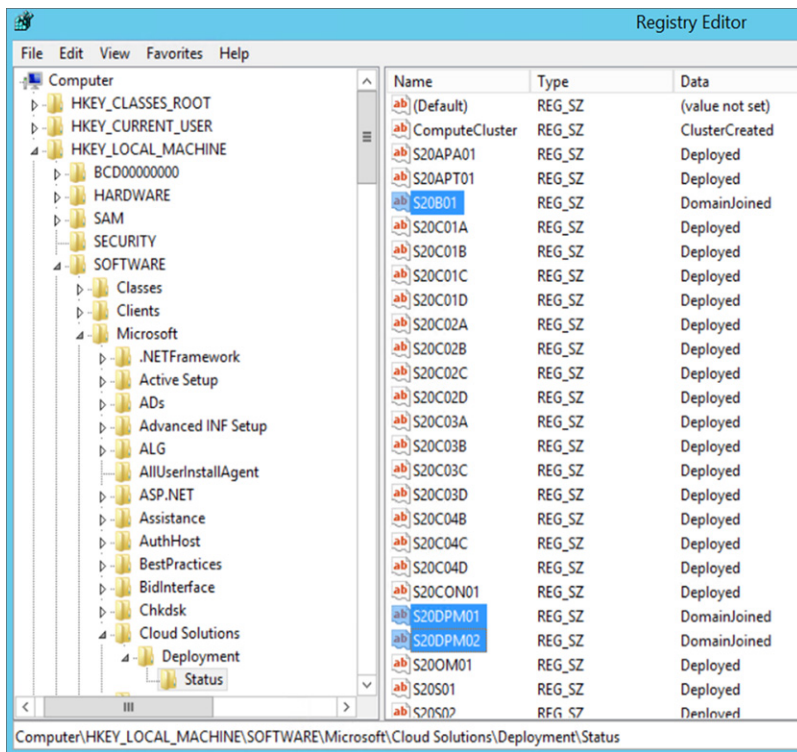


Figure 44. DomainJoined registry key

13 On the Console VM, still logged in as the local administrator, open an elevated Windows PowerShell session and run the following script: "C:\Program Files\Microsoft Cloud Solutions\DeployDriver\BackupDeployDriver\BackupDeployDriver.ps1"

14 If the DPM server backs up the infrastructure VMs, update the server map:

- a Log on to the APA VM—<Prefix>APA01.
- b Open Windows PowerShell.
- c Run the following command, and note the result: (Get-SMAVariable -Name "dpm-configurationmap" -WebServiceEndpoint https://localhost).value.PendingDPMServerMap
- d If the output is null, run the following:

```
$variableName = "DPM-configurationmap"
$a = (Get-SMAVariable -Name $variableName -WebServiceEndpoint https://localhost).value
$a.PendingDPMServerMap = (Get-SMAVariable -Name "dpm-configurationmap" -
WebServiceEndpoint https://localhost).value.DPMServerMap
$a.DPMServerMap = $null
Set-SMAVariable -Name $variableName -value $a -WebServiceEndpoint https://localhost
```

15 Import the DPM disks:

- a Log on to the DPM VM.
- b Open Disk Management—diskmgmt.
You see DPM disks in the **Offline** state (20 disks).
- c Bring all the disks online. (Right-click each disk, and then click **Online**.)
- d Now the disks are all online and in a **Foreign** state. Select any disk, right-click, and then click **Import Foreign Disks**. Do this for all 20 disks.

16 After you import the disks, run the backup Deployment driver script again to correctly update the server map. Run the following command on the console VM (local admin session):

```
"C:\Program Files\Microsoft Cloud Solutions\DeployDriver\BackupDeployDriver\BackupDeployDriver.ps1"
```

17 On the DPM VM, start SQL Server 2014 Management Studio, and do the following:

- a Connect to the DPM server and instance—<DPMName>\MSDPMDB.
- b Restore the DPM database using the backup copy on the E:\ drive of the DPM VM. For more information, see the TechNet Library article [Restore and synchronize the DPM database with DPMSync](#).

- c On the DPM VM, open a command prompt with elevated permissions, and then run the **DPMSync –sync** command. This command restores the old database that has the backup disks added in the storage pool table, but the disks are offline or in an unusable state.
 - d In the DPM Administrator console, open the **Management** workspace, and then click **Disks**.
 - e Right-click each disk, and then click **Remove**.
- 18 On the Console VM, in the VMM console, check the DPM VM properties.
- a In the **VMs and Services** workspace, right-click the DPM VM, click **Properties**, and then click the **Hardware Configuration** tab.
 - b Under **Bus Configuration**, add the pending **<DPMName>-Backup#.vhd** files to the DPM VM. (The VHDs are either in the I:\, J:\, K:\ or L:\, M:\, N:\ volumes of backup host. There should be 20 disks in this format (unless you added more).
- 19 On the DPM VM, in Disk Management (**diskmgmt.msc**), check that all VHDs are in an **Online** state. (If not, right-click, and then click **Online**.)
- 20 In the DPM Administrator console, add the disks to the DPM storage pool. For information about how to do this, see [Configure storage pools and disk storage](#).
- 21 Next, if using Azure Backup, you must configure Azure to allow re-registration of the DPM server to the same backup vault.
- a Sign in to the Azure portal, click **Recovery Services**, and click the backup vault.
 - b Click **Registered Items**.
 - c In the **Type** list, click **Windows Server**.
 - d Select the server that you just recovered, and then click **Allow Re-registration**.

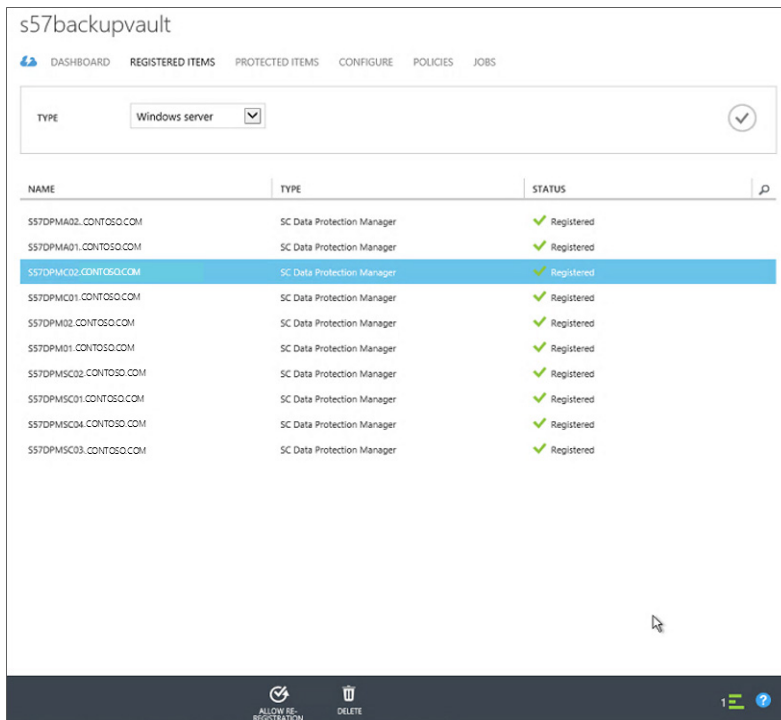


Figure 45. Allow re-registration

- a Download the vault credentials file from the Azure portal to a location on the Console VM, and make sure that you have the passphrase that you used as an encryption key when you opted in to Azure Backup.
 - b In the DPM Administrator console, open the **Management** workspace.
 - c Click **Online**.
 - d On the ribbon, in the **Online Protection** group, click **Register**, and complete the wizard .
 - e Run the **Complete-BackupDeployment** runbook to finish the process.
- 23 After you perform a sync operation, all the data sources should be marked as inconsistent. In the DPM console, trigger a consistency check.
- 24 After all these steps you should be done, with the DPM server up and recovered.

Rebuilding a DPM server

If you determine rebuilding the DPM server is required, do the following:

- 1 Remove the backup host from VMM.
 - a In the VMM console, open the **VMs and Services** workspace.
 - b Under the **All Hosts** host group, remove the backup host on which the DPM VM resides.
- 2 Remove the corrupted DPM server from Operations Manager.
 - a Open the Operations Console.
 - b In the **Administration** workspace, expand **Device Management > Agent Managed**.
 - c Delete the agent on the corrupted DPM server.
- 3 On the Console VM, open Hyper-V Manager and connect to the backup host.
- 4 Delete the corrupted DPM VM.
- 5 Log on to the Console VM by using a local administrator account.
- 6 Update the manifest .XML file for redeployment.

- a Update the backup host configuration. Search for the backup host name in the .xml file, locate the name of the backup host (for example, S20B01) in the <BackupConfiguration> section of the file, and change the **DeploymentStatus** to **"DomainJoined"**.

For example:

```
<BackupConfiguration>
```

```
<Nodes>
```

```
<Node Name="S20B01" DeploymentStatus="DomainJoined" ConfigurationID="828bc360-fd65-4304-bc50-81ea4027ad7f" Password="" SerialNumber="22PGD42">
```

- b Update the DPM node configuration. Search for **<BackupVMs>** in the file. For each DPM server, update **DeploymentStatus** to **"DomainJoined"**.

For example:

```
<BackupVMs>
```

```
<Role Type="DPM" DeploymentStatus="DomainJoined" Name="S20DPM01" BackupHostName="S20B01" ConfigurationID="02651dd9-3028-45a8-9188-9997aa816418" Password="">
```

```
<IPv4Addresses>
```

```
<IPv4Address NetworkId="Management">10.10.20.32</IPv4Address>
```

```
</IPv4Addresses>
```

```
<BackupVhd NumberOfVHDs="20" VhdSize="1024" />
```

```
</Role>
```

```
<Role Type="DPM" DeploymentStatus="DomainJoined" Name="S20DPM02" BackupHostName="S20B01" ConfigurationID="b7a1b6bd-23ff-4f4b-b68e-20ac5e19d005" Password="">
```

- 7 Set the password field in the .xml file for the backup host.
 - a In a Windows PowerShell session, run the following script to set the *\$password* variable to the password you want to set.
\$password = "YourPassword"

```
ConvertTo-SecureString $password -AsPlainText -Force | ConvertFrom-SecureString
```

- b Copy the output of this script.
- c In the .XML file, search for the backup host name, and paste the output from the previous step between the quotes in the `Password=""` field.

<BackupConfiguration>

<Nodes>

```
<Node Name="S20B01" DeploymentStatus="DomainJoined" ConfigurationID="828bc360-fd65-4304-bc50-81ea4027ad7f" Password="PasswordOutput" SerialNumber="22PGD42">
```

For example:

<BackupConfiguration>

<Nodes>

```
<Node Name="S20B01" DeploymentStatus="DomainJoined" ConfigurationID="828bc360-fd65-4304-bc50-81ea4027ad7f"
Password="01000000d08c9ddf0115d1118c7a00c04fc297eb0100000012adbc74a67cfe48ac4404f29b4d43c
c000000002000000000106600000010000200000001565d7d65f0ca2fcf0e0d82f24c481689ccdb7aa4d85
ac400906c7768e6228ba00000000e800000002000020000000750649ad99b3809f7b66f9eb1ff4bb67afa10
8bac79372a56b53ca81ef235c5e30000000eb537f00952fc2d36d3821571b65fc7ccca26066e47eb5de0be691
9a3a24f08e693031d3b8928e1cfa00d32410dfacda40000000e53617e63be31270aled37cb2f54682f802a171
41153741f454be9b3ec7fc6fff1cc0e1a3ca2e56fb7f7af16c5d4a6fd71e0d91c742b38782e03a648c8eb39da
" SerialNumber="22PGD42">
```

- 8 On the Console VM, update the registry subkey for deployment status.
 - a Open **Registry Editor**.
 - b Locate the following registry subkey: **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cloud Solutions\Deployment\Status**
 - c Update the values for the backup host and the DPM VMs from **Deployed** to **DomainJoined**. For example:

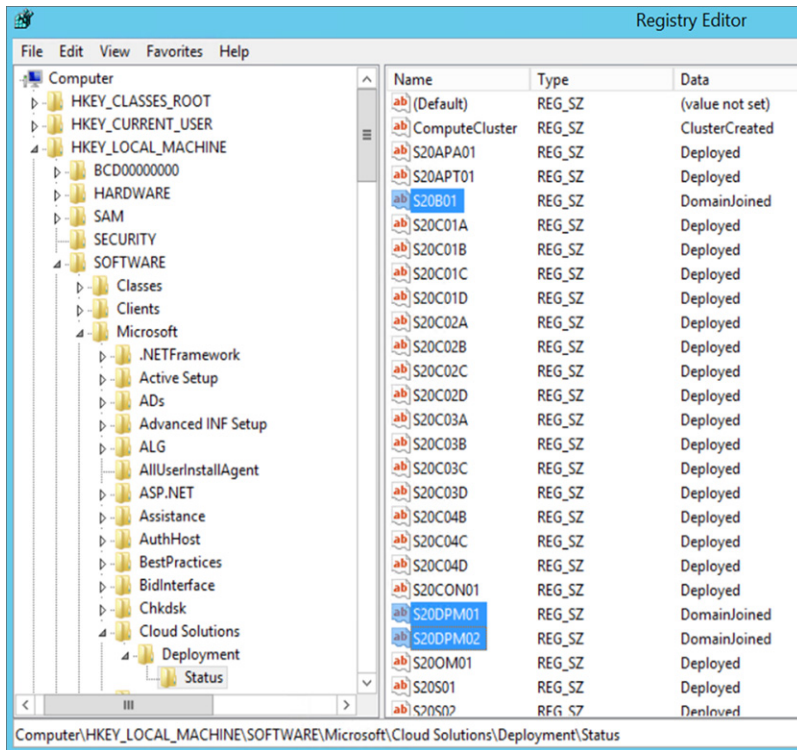


Figure 46. DomainJoined registry key

- 9 On the backup host, open a **Windows PowerShell** session as an elevated user, and then run the following commands to enable the local administrator account, and to update to the same password that you specified for `$password`, in step 7a, that is, the plain text password.


```
net user administrator /active:yes
net user administrator <password>
```

- 10 On the Console VM, still logged in as the local administrator, open an elevated Windows PowerShell session, and run the following script: "C:\Program Files\Microsoft Cloud Solutions\DeployDriver\BackupDeployDriver\BackupDeployDriver.ps1"
- 11 If the DPM server backs up the infrastructure VMs, update the server map.
 - a Log on to the APA VM—<Prefix>APA01.
 - b Start Windows PowerShell.
 - c Run the following command, and note the result: (Get-SmaVariable -Name "dpm-configurationmap" -WebServiceEndpoint https://localhost).value.PendingDPMServerMap
 - d If the command output is null, run the following command:

```
$variableName = "DPM-configurationmap"

$a = (Get-SMAVariable -Name $variableName -WebServiceEndpoint https://localhost).value

$a.PendingDPMServerMap = (Get-SmaVariable -Name "dpm-configurationmap" -
WebServiceEndpoint https://localhost).value.DPMServerMap

$a.DPMServerMap = $null

Set-SMAVariable -Name $variableName -value $a -WebServiceEndpoint https://localhost
```
- 12 To complete the deployment, run the **Complete-Backup** runbook.
- 13 Use the steps in [Recovering a datasource to an alternate DPM server](#) to recover VMs and databases that were protected by the DPM server that was rebuilt.

Recovering the DPM database

- 1 Log on to the DPM VM, and ensure that the backup copies of the DPMDDB database are stored at the path E:\DPMDDBBackup.
- 2 On the DPM VM, open SQL Server 2014 Management Studio. Connect to the DPM server and instance which stores the DPM database that you want to recover (for example, <Prefix>DPM01\MSDPMDB).
- 3 Restore the DPM database by using the backup copy on the E:\ drive of the DPM VM. For more information, see the TechNet Library article [Restore and synchronize the DPM database with DPMSync](#).
- 4 On the DPM VM, open a command prompt with elevated permissions, and then run the **DPMSync -sync** command.
- 5 After the sync operation completes, all the data sources should be marked as inconsistent. In DPM, trigger a consistency check.
- 6 Wait for one scheduled backup to complete. Ensure that previous recovery points exist.

Adding extra disks to DPM

You can use the following procedure if you want to add more VHD disks to the DPM storage pool:

- 1 Use the VMM console to collect the following data:
 - a The DPM VM name.
 - b The volumes on which the DPM backup disks are located. To determine this:
 - 1 In the VMM console, check the DPM VM properties. In the **VMs and Services** workspace, right-click the DPM VM, click **Properties**, and then click the **Hardware Configuration** tab.
 - 2 Under **Bus Configuration**, click each disk to see the locations of the backup VHDs. In the path of the VHDs, look for names in the format <DPMName>Backup#.vhd, and note the drive letter at the beginning of the path. All the VHDs are either I:\, J:\, K:\ or L:\, M:\, and N:\ volumes. Make a note of the volumes that are used.
 - c The number of VHDs that you want to add.
 - d The starting number to use for the new VHDs. To determine this:
 - 1 In the VMM console, click **VMs and Services**.
 - 2 In the **VMs and Services** pane, click **Storage**.

- 3 In the **Disk Information for Virtual Machines** pane, locate and expand the DPM server. If the VMs are not listed, on the **Home** tab of the ribbon, in the **Show** group, click **VMs**.
 - 4 In the list of VHDs that are attached to the DPM server, determine the highest number that was assigned. For example, if the highest number is **<DPMServerName>-Backup20.vhdx**, the starting number for the new VHDs will be **21**.
- 2 Log on to the backup host on which DPM resides.
 - 3 Open a Windows PowerShell session, and run the following command:

 **NOTE: Update the parameter values in the first four lines.**

```
$DPMName = "DPMServerName"

$location = @("I:\","J:\","K:\") #specify the volumes that are used.

$startNumber = 21 #specify the start number for the new disks.

$no_of_vhds = 10 #the number of disks you want to add to DPM.

$DPMVM = get-vm $DPMName

$BackupDiskVHDPaths = @()

$MaxNumberOfControllers = 4

$ExistingVMDisks = $DPMVM.HardDrives.Path

$VhdsToBeAdded2VM = @()

#create VHDs

for($i=0;$i -lt $no_of_vhds;$i++)
{
    $diskNum = $i + $startNumber ;

    $path = $location[$i%3];

    $vhddpath = "$path$DPMName-Backup$diskNum.vhdx"

    $vhdsSize = 1024GB

    New-VHD -Path $vhddpath -Dynamic -SizeBytes $vhdsSize

    $BackupDiskVHDPaths += $vhddpath
}

$VhdsToBeAdded2VM = $BackupDiskVHDPaths

#VHDsOnBus contains the existing VHDs count for bus(index of array)

$VHDsOnBus = @{}

for($Bus = 0; $Bus -lt $AdaptersCount; $Bus++)
{
    $VDDs = $DPMVM.hardDrives | where{$_ .ControllerNumber -eq $Bus -and $_ .ControllerType -eq
"SCSI"}
```

```

if($VDDs -ne $null)
{
$VHDsOnBus[$Bus] = $VDDs.Count
}
else
{
$VHDsOnBus[$Bus] = 0
}
}

#Add VHDs to VM

foreach($VhdTobeAdded in $VhdsToBeAdded2VM)
{
#Find the bus with minimum number of VHDs attached

$Bus = ($VHDsOnBus.GetEnumerator() | Sort-Object -Property value)[0].key

Add-VMHardDiskDrive -VM $DPMVM -ControllerType SCSI -ControllerNumber $Bus -Path
$VhdTobeAdded

$VHDsOnBus[$Bus] += 1
}

```

- 4 After the disks are created, connect to the DPM VM, and initialize the disk by using Disk Manager.
- 5 Add the disks to the DPM storage pool. For information about how to do this, see [Configure storage pools and disk storage](#).

Monitoring DPM

DPM automatically backs up data according to the backup settings.

At times, DPM backups might fail. For example, a communication failure may occur with the SQL Servers, the SQL Servers may not be running, or there may be other connection issues.

Dell recommends that you regularly monitor DPM. Dell Hybrid Cloud System for Microsoft installs DPM, the DPM Central Console, and the management pack that is integrated with Operations Manager. You can monitor all failure alerts in Operations Manager. To do this:

- 1 Log on to the Console VM by using an account that is a member of the **<Prefix>Ops-Admins** group.
- 2 Open the Operations Console.
- 3 In the Monitoring workspace, expand **System Center 2012 R2 Data Protection Manager** to see the Alert and State views and any associated alerts.

NOTE: The DPM Central Console is integrated with Operations Manager (and does not show up as a separate interface). It enables you (through the System Center 2012 R2 Data Protection Manager node) to monitor all DPM servers, and to take actions in response to alerts. For more information, see the following topics in the TechNet Library:

- [Monitor DPM](http://technet.microsoft.com/library/jj628024.aspx) (http://technet.microsoft.com/library/jj628024.aspx)
- [Manage multiple DPM servers with Central Console](http://technet.microsoft.com/library/jj860391.aspx)(http://technet.microsoft.com/library/jj860391.aspx)

As described in [Recovering DPM from DPM failures](#), recovering a DPM server includes leveraging DPM database backups. Each DPM server is configured as follows:

- Backs up the DPM database to the E:\ drive on the same VM.
- Scheduled to back up the database every four hours by using the Windows **DPMDBBackup** Task Scheduler job.

Because this backup job can fail for many reasons, you should regularly monitor the status of this job on all DPM servers. The most common possible failures include the following.

Table 29. Backup failures

Issue	Symptom	Resolution
The request to SQL Server to export and copy the DPM database to the E:\ drive fails.	Event Viewer displays a SQL Server database error.	Fix the SQL Server error, and then run the DPMDBBackup job again.
Drive E:\ runs out of space.	Event Viewer displays a Disk Full error.	Delete the oldest file on the E:\ drive (and make a copy if necessary). Then, run the DPMDBBackup job again.

Using the Dell Hybrid Cloud System for Microsoft data consistency runbooks

Dell Hybrid Cloud System for Microsoft includes runbooks that you can use to detect and, in some cases, to automatically recover from data inconsistencies between the databases of the components that are deployed as part of Dell Hybrid Cloud System for Microsoft. Specifically, the **Invoke-DataConsistency** runbook (and its associated child runbooks) detects and tries to recover from inconsistencies between components' states.

Dell recommends that you use the Dell Hybrid Cloud System for Microsoft data consistency runbooks for detection and recovery after you restore a management component database from backup. For example, you may have restored a database to fix data corruption. The detection runbooks can report inconsistencies between the Windows Azure Pack, SPF, and VMM database components, that is, objects associated with the VM Cloud Resource Provider.

The detection runbooks can report inconsistencies between the Windows Azure Pack, SPF, and VMM database components, that is, objects associated with the VM Cloud Resource Provider.

Overview of the data consistency master and child runbooks

The data consistency runbooks include a master runbook, which in turn triggers a set of child runbooks.

The master runbook, **Invoke-DataConsistency**, is the main runbook to use for detection and recovery. When you run it, you must specify a subsystem. This triggers the associated child runbooks for that subsystem. To understand what the subsystem targets, see the information in the following table.

Table 30. Data Consistency Runbooks

Subsystem	Detection and Recovery Child Runbooks
Virtual Machine Provider (VMProvider)	<p data-bbox="743 264 1193 289">Detection: Test-VmCloudsDataConsistency</p> <p data-bbox="743 319 1485 422">Detects and reports inconsistencies between the Windows Azure Pack, SPF, and VMM database components, that is, objects associated with the VM Cloud Resource Provider. This runbook can detect the following issues:</p> <p data-bbox="743 451 847 476">For VMM:</p> <ul data-bbox="743 506 1477 646" style="list-style-type: none"> • "Object not found" for cloud, hardware profile, VM network, VM template, and user role • "Out of sync" for user role quota, user role network settings, and user role virtual machine permissions • Other – Logical networks not added to the cloud. <p data-bbox="743 676 836 701">For SPF:</p> <ul data-bbox="743 730 1362 779" style="list-style-type: none"> • "Object not found" for the Gallery item, stamp, and tenant • "Out of sync" for tenant status <p data-bbox="751 808 1453 890">NOTE: Out of sync indicates that the properties in the component are out of sync with the properties that are set on the plan, subscription, or add-on.</p> <p data-bbox="743 919 1214 945">Recovery: Repair-VmCloudsDataConsistency</p> <p data-bbox="743 974 1433 1037">Tries to automatically recover issues with plans, add-ons, and subscriptions. Also reports issues that the runbook cannot fix, where manual recovery may be required.</p>

NOTE: There is an extra data consistency runbook that is not called by the `Invoke-DataConsistency` runbook. This is the `SyncVMCloudsWithFabric` runbook. It refreshes fabric objects such as VMM hosts, clusters, library shares, virtual machines, and so on, to bring the VMM database to a consistent state with the current state of the underlying fabric. After a fabric sync completes, the runbook syncs VMM with Operations Manager. Typically, you should not have to run this runbook because VMM includes refreshers that do this automatically. If you run this runbook, *be aware that it affects performance, and it can take several hours to complete*, depending on the number of VMs. You would run this only if you restored the VMM or Operations Manager database, and issues were not automatically fixed by the VMM refresher.

How to use the data consistency runbooks

This section describes the recommended way to run the detection and recovery runbooks.

You can run the `Invoke-DataConsistency` runbook, both detection and recovery, when there is live traffic on the system. However, you must first run a script to reset the passwords across the system. This procedure requires downtime of the whole stamp.

Depending on the output of the detection process, you must either run the `Invoke-DataConsistency` runbook again with the repair option enabled, and/or perform extra manual steps.

- 1 **Create a shared folder for the output record.** Before you begin, make sure that a shared folder exists that you can specify as the location to store the output report. You must grant the `<Prefix>System` account Read and Write permissions to the share.
 - a Create a folder on the Console VM, such as `DCOutput`.
 - b Right-click the folder, and then click **Properties**.
 - c Click the Sharing tab, and then click Advanced Sharing.
 - d Select the Share this folder check box, and then click **Permissions**.
 - e Click Add, enter the account `<Prefix>System`, and then click **OK**.
 - f Click the account that you just added, and then under **Allow**, select the **Change** check box.

- g Click **Apply**, click **OK** two times, and then click **Close**.
- 2 **Run the password reset script.** After you restore any of the following databases, run the password reset script as described in [How to run the MCPASSWORDReset script](#):
- Operations Manager database
 - VMM database
 - SMA database
 - SPF database
 - Any of the Windows Azure Pack databases
- 3 **Run the database consistency runbooks.**
- a In the Windows Azure Pack management portal for administrators, run the **Configure-DataConsistency** runbook. You only have to run this runbook one time—the first time that you use the data consistency runbooks.
 - b Run the **Invoke-DataConsistency** runbook to detect inconsistencies. You can run this when there is live traffic on the system. However, with live traffic, detection may take longer. Specify the following parameter values:

Table 31. Parameter values for Invoke-DataConsistency runbook

Parameters	Value
AllowRepair	No
ReportDestination	Enter the UNC share path of the destination to store the output report, for example \\<Prefix>CON01\DCOutput. This is the share that you created earlier.
Subsystem	VMPProvider

- c When detection finishes, you can view the output report at the destination that you specified for **ReportDestination**. The report looks similar to the following:

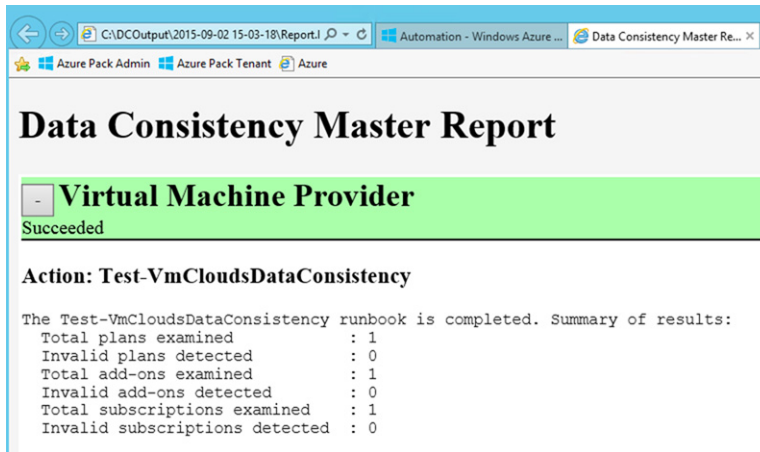


Figure 47. Data Consistency Master Report

The report indicates a status of either "Succeeded" or "Inconsistencies Detected."

- d If there are inconsistencies that were detected, expand the category for more details. To repair inconsistencies, do the following:

NOTE: You can run repair operations when there is live traffic on the system. However, with live traffic, repair may take longer.

- To perform automatic recovery of as many issues as possible, run the **Invoke-DataConsistency** runbook with *AllowRepair* set to **Yes**, and *Subsystem* set to **VMPProvider**.
- For issues that cannot be automatically recovered, see the following section of this guide, [Troubleshooting data consistency issues](#).

Troubleshooting data consistency issues

There are some issues that the data consistency runbooks cannot automatically repair.

This section provides troubleshooting steps that you can follow to try to resolve these issues. If troubleshooting steps are not listed or do not resolve the issue, contact support.

Troubleshooting steps are organized by report categories. In addition, there is information about how to manually recover access to tenant-created objects.

Table 32. Virtual Machine Provider

Error	Cause/Resolution
Cloud not found in VMM	<p>Cause: This issue occurs if a Windows Azure Pack plan is configured with a cloud, but the cloud does not exist in VMM.</p> <p>Resolution: Follow these steps as a VMM administrator:</p> <ol style="list-style-type: none">1 In the VMM console, verify that a valid cloud exists, or create a cloud if applicable.2 In the Windows Azure Pack management portal for administrators, open the plan properties.3 Select a valid cloud.4 Save the plan settings.
StampCannotBeFound = The SPF stamp {0} cannot be found. This issue is not automatically recoverable.	<p>Cause: This issue occurs if the stamp that is referenced by a Windows Azure Pack plan no longer exists in the SPF database. This would only occur if the stamp ID was manually deleted in the SPF database.</p> <p>Resolution: Restore the SPF database to the last known good state.</p>

How to manually recover access to tenant-created objects

The consistency scripts do not detect or recover tenant-created objects. These include VM networks, VMs, and VM roles. If a tenant loses access to a tenant-created object, you can restore access by using VMM cmdlets in the VMM command shell. You can also recover access to a tenant-created VM role.

You can use the Console VM to perform all procedures in this section. You must be logged on as a VMM administrator (i.e. a member of **<Prefix>Ops-Admins**).

Before you perform any of these procedures, run the following cmdlets to get the VMM server connection and to assign the following variable, where **\$ur** is the VMM user role object for the tenant:

```
Get-SCVMMServer -ComputerName <Prefix>VMM01 -ForOnBehalfOf  
$ur = Get-SCUserRole -ID <SubscriptionID>  
$cloud = Get-SCCloud -Name "<Cloud Name>"
```

NOTE: *<SubscriptionID>* is the subscription ID of the tenant. You can obtain the subscription ID in the Windows Azure Pack management portal for administrators.

Restoring access to a tenant-created virtual machine

To restore a tenant's access to virtual network (**\$vmn**), run the following commands, where `<VMNetworkName>` is the name of the tenant's virtual network, and `<user1@domain.com>` is the tenant's user account:

```
$vmn = Get-SCVMNetwork -Name <VMNetworkName>
Set-SCVMNetwork -VMNetwork $vmn -UserRole $ur -Owner <user1@domain.com>
-Cloud $cloud
```

Recovering access to a tenant-created VM role

To recover access to a tenant-created VM role, the VM role must be healthy and have all of its associated VMs. Also, the VMM host must not have been removed and re-added in VMM. To recover access to the VM role, run the following command, where `<VMRoleName>` is the name of the VM role, and `<user1@domain.com>` is the tenant's user account:

```
Set-CloudService -CloudService <VMRoleName> -Owner <user1@domain.com> -UserRole $ur -Cloud $cloud
```

Updating the Dell Hybrid Cloud System for Microsoft

The following sections describe how you can apply software and firmware updates for the Dell Hybrid Cloud System for Microsoft stamp, using the Patch and Update framework.

Overview of the Patch and Update framework

Use the Patch and Update framework to apply software and firmware updates.

Throughout the lifecycle of the Dell Hybrid Cloud System for Microsoft, there are software, driver, and firmware updates that either address issues or provide for enhanced operations. Dell releases Patch and Update (P&U) bundles to make it easier to maintain the cloud solution. These bundles ensure that the process of applying updates is minimally disruptive to the solution and the virtual machines that it is hosting. The bundles are available from [Support.dell.com](https://support.dell.com), and combine the relevant software, driver, and firmware updates from both Dell and Microsoft into a single package. This package is extracted and run from within the Dell Hybrid Cloud System for Microsoft, and takes advantage of technologies that enable you to apply the updates in an orchestrated manner. Individual nodes or functions within the cloud solution may be unavailable during the update process, but the virtual machines that the solution is hosting remain operational. When these bundles are released, there are Release Notes to describe their contents and instructions that outline how to extract and apply the Patch and Update bundle within the cloud solution.

⚠ WARNING: The addition of any non-DHCS hardware to your system will cause the Patch and Update process to fail.

ℹ NOTE: The P&U framework does not update tenant VMs.

When the P&U framework runs, it does the following:

- Orchestrates the updates so that they are performed in the correct order.
- Automatically puts servers in and out of maintenance mode during servicing.
- Validates components when servicing is complete.

The P&U framework installs approved software updates on infrastructure hosts and VMs for various combinations of the following products:

ℹ NOTE: Any given package may or may not contain updates from all the categories listed. For the specific contents of any particular package, see the package *Release Notes*, which you can obtain from the same download location as the package itself. See [How to obtain the update packages](#) for details.

- Windows Server

- Windows Azure Pack
- System Center
- SQL Server
- Dell software
- Dell Deployment UI
- Drivers and firmware updates for Dell Hardware

If the package also includes firmware and driver updates, the framework installs the approved firmware and driver updates on the physical cluster nodes.

IMPORTANT: Do NOT install Windows Server, Windows Azure Pack, System Center, and SQL Server updates by using any method other than the P&U framework. Install only update packages that Microsoft and Dell have tested and approved for the Dell Hybrid Cloud System for Microsoft.

Note the following:

- The P&U update process is the only supported process to apply the Microsoft updates to DHCS.
- Applying Dell EMC firmware or updates for individual components, and not via the Dell P&U package, is known to cause technical issues.
- To be fully supported, the customer must apply all P&U updates on a regular basis.

How to check which update package is installed

To check the version of the update package that is currently installed on the stamp, do the following:

- 1 On the Console VM, open the DeploymentManifest.xml file at the path:
C:\Program Files\Microsoft Cloud Solutions\DeployDriver\Manifests
- 2 At the top of the file, look for the following entries:
 - **"Version="**: This is the version of the Dell-provided update package.
 - **"MicrosoftVersion="**: This is the version of the Microsoft-specific updates that were incorporated in the Dell-provided update package, for example:
"MicrosoftVersion": "1.0.1603.21000"

The third value (**1603** in the example) indicates the year and month of the Microsoft update package.

How to obtain update packages

Dell releases approved updates as Dell Hybrid Cloud System for Microsoft P&U packages. To check if a new update package is available, see the **Drivers and Downloads** section of the **Dell Hybrid Cloud System for Microsoft** page on the Dell Support website—support.dell.com. Navigate to **Browse for a product**. Click **View products**. Click **Servers, Storage, & Networking > Engineering Solutions > Microsoft Cloud Solutions > Dell Hybrid Cloud System for Microsoft**. You can find the latest update package by clicking **Drivers and Downloads**.

Starting with release 1.1.1, update-specific detailed instructions for the Patch and Update process are distributed as part of the update package. You can find the current document, titled *DHCS Patch and Update Framework for 1703*, at the location where you find approved updates, as described in the preceding paragraph.

Shutting down and starting up the stamp

There are scenarios where a graceful shutdown of the Dell Hybrid Cloud System for Microsoft stamp may be required. To do this, you must follow a series of sequenced steps. In addition, the case of a power outage is covered at the end of this section.

Before you begin

To perform a graceful shutdown of the Dell Hybrid Cloud System for Microsoft stamp you must follow this sequence:

- The cluster names and IP addresses for the compute cluster, Scale-Out File Server (SOFS), and SQL Server guest cluster
- Host names and IP addresses for the compute cluster, storage cluster, and SQL Server guest cluster
- Infrastructure VM names and IP addresses.

For information about how to collect this information by using Windows PowerShell, see [Appendix C: Commands to retrieve cluster names, host names, and IP addresses](#).

You can perform shutdown and startup processes from the Console VM with an account that is a member of the **<Prefix>-Setup-Admins** security group.

It is recommended that you read this entire section before you shut down the stamp to familiarize yourself with the steps involved.

Unless otherwise noted, for any instruction where you must open a Windows PowerShell session or the command prompt, open these tools with elevated user rights; that is, started with the **Run as Administrator** option.

Shutting down the stamp

At a high level, shutdown steps are as listed below. Detailed instructions for each step are in the sections that follow:

- 1 If the Dell Hybrid Cloud System for Microsoft backup infrastructure is in place, check and stop any running backup jobs.
- 2 Shut down DPM VMs.
- 3 Shut down the backup hosts.
- 4 Shut down tenant VMs.
- 5 Shut down all infrastructure VMs except for the Console VM.
- 6 Shut down the compute cluster hosts.
- 7 Shut down the file server cluster hosts.
- 8 Optionally, turn off the JBODs. However, this requires physical presence.
- 9 Optionally, unplug the network switches. This also requires physical presence.
- 10 Turn off power to the stamp (the power distribution units or PDUs).

Use the following detailed procedures to gracefully shut down the stamp.

Preparing a laptop if iDRACs are connected

If the integrated Dell Remote Access Controllers (iDRACs) are connected in the environment, Dell recommends using a laptop to perform these tasks.

To prepare the laptop:

- 1 Connect the laptop to port 39 or 40 of the switch for the Dell Hybrid Cloud System for Microsoft stamp. This switch is the network switch that you use for management of Dell Hybrid Cloud System for Microsoft infrastructure components through iDRAC connections.
- 2 Configure the laptop with a static IP address from the iDRAC subnet range.
This step enables network communication to the iDRACs in the Dell Hybrid Cloud System for Microsoft stamp.
- 3 Install Java version 7—or a later version—on this laptop so that you can start the virtual console through the iDRAC interface.

Step 1: Stop any backups

NOTE: Dell recommends that any infrastructure VM and database backups that may be in progress are completed before you shut down the infrastructure VMs. For information about the default schedule, see [Default backup and retention policy](#).

- 1 Log on to the Console VM (<Prefix>CON01) using an account that is a member of the <Prefix>-Ops-Admins group.
- 2 Open the Operations console.
- 3 In the **Monitoring** workspace, expand **System Center 2012 R2 Data Protection Manager**, expand **State views**, and then click **DPM servers**.
- 4 In the **Tasks** pane, under **DPM Server Tasks**, click **View Jobs**.
In the **View Jobs** dialog box, you can see a consolidated view of all jobs for all DPM servers in the stamp.

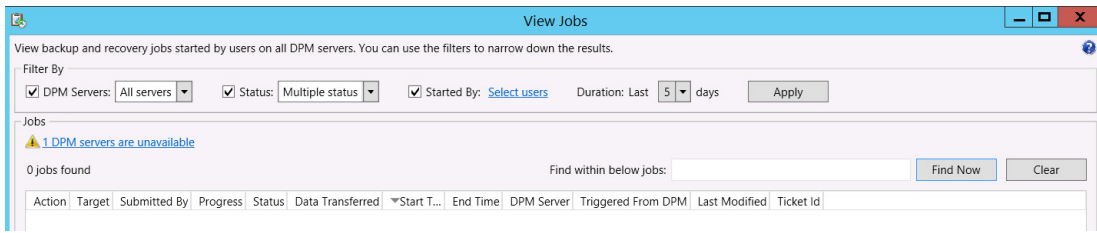


Figure 48. View backup jobs

- 5 You can either wait for the jobs to complete, or click **Cancel Jobs**.

For more information, see [Using Central Console to administer DPM](http://technet.microsoft.com/library/jj860391.aspx) in the TechNet Library (<http://technet.microsoft.com/library/jj860391.aspx>).

Step 2: Shut down DPM VMs

From the Console VM, log on to each DPM VM, and shut down the VM.
To connect to a DPM VM, you can use Hyper-V Manager or the VMM console. To connect by using the VMM console:

- 1 In the VMM console, open the **VMs and Services** workspace.
- 2 Expand **All Hosts**, and then locate and click the backup host.
- 3 In the VMs pane, right-click a DPM VM, point to **Connect or View**, and then click **Connect via Console**.

Step 3: Shut down the backup hosts

Next, shut down the backup hosts using one of the two following methods.

- 1 **Method 1: Use the Stop-Computer cmdlet.**
 - a Log on locally to a backup host with an account that is a member of the <Prefix>-Ops-Admins group.
 - b Open Windows PowerShell, and run the following command:
Stop-Computer -Force
 - c After the host shuts down, continue to the next backup host. Repeat these steps until all backup hosts are shut down.

- 2 **Method 2: Connect through the iDRACs**

If the iDRACs are connected, you can use the following method to shut down the backup hosts:

- a From a laptop that is connected to port 39 or 40 of the switch, use a web browser to connect to the IPv4 iDRAC address of the first backup host. For example, open <https://192.168.164.150>.
- b In the portal, expand **Overview-Server-Power/Thermal**, click the **Power Control** tab, click **Graceful Shutdown**, and then click **Apply**.

- c Repeat these steps to shut down each backup host.

Step 4: Shut down the tenant VMs

- 1 Log on to the Console VM using an account that is a member of the **<Prefix>-Setup-Admins** group.
- 2 Open Failover Cluster Manager, right-click **Failover Cluster Manager**, click **Connect to Cluster**, click **Browse**, and then click the compute cluster.
- 3 Under the cluster name, click **Roles**, sort the VMs by name, and select all **VMs** except the following ones (the infrastructure VMs):
 - <Prefix>APA01
 - <Prefix>APT01
 - <Prefix>CON01
 - <Prefix>OM01
 - <Prefix>SQL01
 - <Prefix>SQL02
 - <Prefix>VMM01
- 4 Right-click the selection, and then click **Shut Down** to shut down all the tenant VMs.

Step 5: Shut down infrastructure VMs

After you ensure that any backups that are running on the management infrastructure VMs are complete, follow these steps to shut down specific infrastructure VMs in a specific order:

- 1 Connect to the Console VM using an account that is a member of the **<Prefix>-Setup-Admins** group.
- 2 Open **Failover Cluster Manager**, right-click **Failover Cluster Manager**, click **Connect to Cluster**, click **Browse**, and then click the compute cluster.
- 3 Under the cluster name, click **Roles**, and sort the VMs by name.
- 4 Shut down the following infrastructure VMs in the following order. To shut down a VM, right-click the VM, and then click **Shut Down**.
 - a <Prefix>APA01
 - b <Prefix>APT01
 - c <Prefix>OM01
 - d <Prefix>VMM01
- 5 In Failover Cluster Manager, connect to the **<Prefix>SQLCL** cluster.
- 6 Click **Roles**. There should be two roles listed (SQLIN01 and SQLIN02).
- 7 Right-click each role, and then click **Stop Role**.
- 8 After you have completed this, and while still in Failover Cluster Manager, connect to the compute cluster.
- 9 Shut down the following running VMs one at a time. To do this, right-click a VM, and then click **Shut Down**.
 - a <Prefix>SQL01
 - b <Prefix>SQL02
- 10 Close Failover Cluster Manager.
- 11 At this point only the **<Prefix>CON01** VM will be running. This represents the desired state at shutdown time.
- 12 Disconnect from the Console VM.

Step 6: Shut down the compute cluster hosts

Next, you must shut down the compute cluster hosts. There are two methods that you can use to perform this operation.

- 1 **Method 1: Use the Stop-Computer cmdlet**
 - a Log on to any domain-joined computer, external to the stamp, with an account that is a member of the **<Prefix>-Ops-Admins** group.
 - b Open an elevated Windows PowerShell session.

- c To stop the remote computer, run the following command where *<HostName>* is the name of a compute cluster host:
Stop-Computer -ComputerName <HostName> -Force
- d When the host is shut down, continue to the next host. Always wait until the current host shuts down before you shut down the next host. Continue until all compute cluster hosts are shut down.

2 Method 2: Connect through the iDRAC

If the iDRACs are connected, you can use the following method to shut down the compute cluster hosts:

- a Using the laptop that is connected to port 39 or 40 of the switch, connect to the IPv4 iDRAC address of a compute cluster host by using a browser—for example <https://192.168.164.133>.
- b Expand **Overview-Server-Power/Thermal**. Click the **Power Control** tab. Click **Graceful Shutdown**, and then click **Apply**.
- c Repeat for every compute cluster on the stamp.

Step 7: Shut down the file server cluster hosts

Finally, shut down the file server cluster hosts. You can follow the same procedure as in the previous step, except specify the file server cluster host names or iDRAC IP addresses. Make sure that you shut down the hosts one at a time.

Step 8: Shut down other hardware devices

At this point, the JBODs are still powered on and are not remotely manageable in terms of power on/off.

Depending on the reason for the stamp shutdown (maintenance versus relocation), you can do either of the following:

- Power them off by switching off the PDUs for the rack, or
- Switch them off individually. Press the on/off switch on the back of the device.

Starting up the stamp

At a high level, the Dell Hybrid Cloud System for Microsoft startup sequence steps are as follows:

- 1 Power Distribution Units (PDUs)
- 2 JBODs
- 3 File server cluster hosts
- 4 Compute cluster hosts
- 5 Infrastructure VMs
- 6 Tenant VMs
- 7 Backup hosts
- 8 DPM VMs

Use the following detailed procedures to gracefully start up the stamp.

Prerequisites

Prepare a laptop if iDRACs are connected

If the iDRACs are connected in the environment, Dell recommends that you use a laptop to perform these tasks.

- 1 Connect the laptop to port 39 or 40 of the switch of the Dell Hybrid Cloud System for Microsoft stamp. This switch is the network switch that you use for management of Dell Hybrid Cloud System for Microsoft infrastructure components through iDRAC connections.
- 2 Configure the laptop with a static IP address from the iDRAC subnet range. This step enables network communication to the iDRACs in the Dell Hybrid Cloud System for Microsoft stamp.

- 3 Install Java version 7 on this laptop so that you can start the virtual console through the iDRAC interface.

Ensure that AD DS services are available

Ensure that your Active Directory Domain Services (AD DS) infrastructure is available, and functional.

Step 1: Power on the hardware devices

- 1 Power on the PDUs.
- 2 Ensure the on/off switch is on for the JBODs.

Step 2: Power on the file server cluster hosts

- 1 Power on the file server cluster hosts by using either of the following methods:
 - Use the on/off switch on the front of the server, or
 - If the iDRACs are connected, connect to the IPv4 iDRAC address of the host from the laptop that is connected to port 39 or 40 of the switch by using a browser, for example, open <https://192.168.164.131>.
- 2 Expand **Overview-Server-Power/Thermal**. Click the **Power Control** tab. Click **Power on System**, and then click **Apply**.
- 3 Ping the file server cluster hosts until they respond. It might take 10-20 minutes for them to be reachable.
- 4 When the file server cluster hosts start responding, use the iDRAC to connect to one of the hosts and start a virtual console. Log on with an account that is a member of the **<Prefix>-Ops-Admins** group, open Windows PowerShell, and then run the following commands:
 - a **Get-StorageEnclosure** to verify that all enclosures are online.
 - b **\$p = Get-PhysicalDisk** followed by **\$p.count**.
 - c **Get-StoragePool** to verify that the pool has been discovered and to view its health state.
 - d **Get-VirtualDisk** to verify whether all the storage spaces are online.

After you verify that the storage is running and healthy, continue to the next step.

Step 3: Power on the compute cluster hosts

- 1 Power on the compute cluster hosts by using either of the following methods:
 - The on/off switch on the front of the server, or
 - If the iDRACs are connected, connect to the IPv4 iDRAC address of the hosts by using a browser, for example, <https://192.168.164.133>, on the laptop that is connected to port 39 or 40 of the switch.
- 2 Ping the compute cluster hosts until they respond. It may take 10-20 minutes for them to be reachable.

Step 4: Power on the infrastructure VMs and tenant VMs

Use Remote Desktop Connection to connect to the Console VM with an account that is a member of the **<Prefix>-Setup-Admins** group.

ⓘ | NOTE: You might have to wait an hour or longer from the time you turned on the compute cluster hosts to perform this step.

- 1 Open Failover Cluster Manager.
- 2 Connect to the compute cluster.
- 3 Click **Roles**. Check the state of the VMs. The **<Prefix>CON01** VM should be running.
- 4 From Failover Cluster Manager, start the following infrastructure VMs:
 - a **<Prefix>SQL01**
 - b **<Prefix>SQL02**
- 5 Wait until the VMs in the SQL Server guest cluster are in a **Running** state.
- 6 From Failover Cluster Manager, connect to the SQL Server guest cluster (**<Prefix>SQLCL**.) Click **Roles**, and verify that both instances (SQLIN01 and SQLIN02) are online. If not, right-click the role, and then click **Start Role**.

- 7 After all SQL Server instances are online, in Failover Cluster Manager, connect back to the compute cluster, and start the remaining infrastructure VMs in the following order:
 - a <Prefix>VMM01
 - b <Prefix>OM01
 - c <Prefix>APA01
 - d <Prefix>APT01
- 8 In Failover Cluster Manager, while connected to the compute cluster, ensure you select all tenant VMs and start them as well.
- 9 Clear rule-based generated alerts that were created during the startup process. To do this, open the Operations Manager Shell from the Console VM, and run the following commands:


```
$InstanceObject = Get-SCOMClass -Name Microsoft.SystemCenter.ManagementServersGroup | Get-SCOMClassInstance | Get-SCOMMonitoringObject

Start-SCOMTask -Task (Get-SCOMTask -Name Microsoft.Cloud.Overrides.Tasks.ResolveAlertsPerMP) -Instance $InstanceObject
```

Step 5: Validate the stamp

- 1 On the Console VM, open the Operations console.
- 2 In the **Monitoring** workspace, expand **Microsoft Cloud Dashboard**, and then click **Microsoft Cloud Dashboard**.
- 3 Make sure all components are healthy.
See [Known issues](#) for any expected issues and their resolution steps.

Ensure that the Windows Azure Pack portals are working.

The Windows Azure Pack portals depend on a security token service such as AD FS or an external third-party identity system for your domain.

Make sure that you can access the Windows Azure Pack management and tenant portals.

Step 6: Power on the backup hosts

After the entire stamp is powered up, start all the backup hosts. Follow these steps:

- 1 Power on the backup hosts by using either of the following methods:
 - Use the on/off switch on the front of the server.
 - If the iDRACs are connected, connect to the IPv4 iDRAC address of the hosts by using a browser, for example <https://192.168.164.150>, on the laptop that is connected to port 39 or 40 of the switch.
- 2 Verify that each DPM server can communicate with all the compute hosts. To do so, perform the following steps:
 - a Log on to the Console VM with an account that is a member of the **<Prefix>-Setup-Admins**.
 - b Open the DPM Administrator console, and then open the **Management** workspace.
 - c On the ribbon, in the **Agents** group, click **Refresh** to refresh all agents.

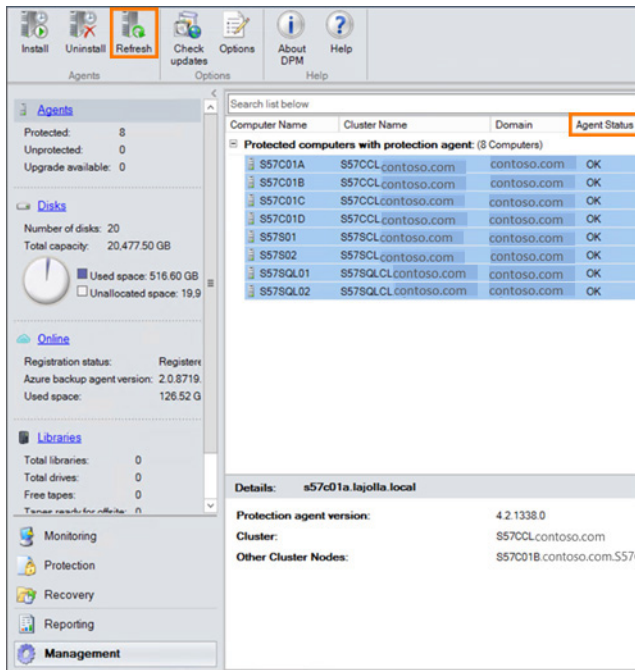


Figure 49. DPM Refresh agents

Known Issues

Issue #1: WAP (Windows Azure Pack) Admin API, WAP Usage, and Usage Collector components report a Warning state.

Symptoms: After a restart of Dell Hybrid Cloud System for Microsoft, the following Windows Azure portal components are in a **Warning** state, and there are the following alerts in Operations Manager:

- Windows Azure Pack Site Unknown Error Monitor Usage
- Windows Azure Pack Site Unknown Error Monitor Usage Collector.

Possible cause:

At some point during the startup, the Windows Azure management portal for administrators VM (<Prefix>APA01) could not connect to the Windows Azure Pack database.

Resolution:

No action is required. Wait for 1 hour for the monitors to automatically reset the state to healthy.

Issue #2: During a restart of Dell Hybrid Cloud System for Microsoft, startup of the compute cluster nodes leaves one or more of the compute cluster hosts in a **Needs Attention** state in VMM. However, the host is actually running.

Symptoms:

- In the VMM console, the following status is reported for the compute cluster host and its VMs:
 - **Host Status** of the compute cluster node is **Needs Attention**.
 - VMs running on the computer cluster host have a status of **Host Not Responding**, and the virtual machine state is **Stopped**.
- In Failover Cluster Manager, the compute cluster host and the VMs that are on it are in a **Running** state.

Resolution:

- 1 From the Console VM, open Event Viewer, connect to the cluster node that needs attention remotely, and **Save All Events As**.
- 2 Open the VMM console, open the **Jobs** workspace, and check for failed **Refresh host cluster** jobs.
- 3 In the error details for each of the failed jobs, check for the following error:

Error (2912)

An internal error has occurred trying to contact the <Server_FQDN> server:
: .

WinRM: URL: [http://<Server_FQDN>:5985], **Verb:** [ENUMERATE],
Resource: [http://schemas.microsoft.com/wbem/wsman/1/wmi/root/cimv2/
Win32_AssociatedProcessorMemory],
Filter: []

Unknown error (0x80041013)

- 4 On the Console VM, open a command prompt, and run the following command to find out whether any of the WinRM errors still persist:

```
Gwmi -class "Win32_AssociatedProcessorMemory" -ComputerName "ServerName"
```

- 5 If the issue persists, collect Application and System event logs, and then restart the compute cluster host.

The restart initiates autorefresh jobs in VMM, which refresh the status of the host and VMs running on the host.

NOTE: VMM automatically refreshes the status of clustered hosts and VMs at these intervals:

- A **Refresh host cluster** job runs every 30 minutes.
- A **Refresh virtual machine** light refresh job runs once every hour.

Recovering after a power outage

There are occasions where a power outage may cause the Dell Hybrid Cloud System for Microsoft stamp to shut down unexpectedly. When power becomes available again, the stamp will power on automatically without any manual intervention.

The following hardware devices will power on immediately:

- JBODs.

The following hardware components will power on with a delay of 1-10 minutes:

- 1 File server cluster hosts
- 2 Compute cluster hosts

Approximately 2 hours after power up, the stamp is expected to be in a functional state. You must perform the following steps 2 hours after power up.

Prerequisites

Prepare a laptop if iDRACs are connected.

If the iDRACs are connected in the environment, Dell recommends that you use a laptop to perform these tasks:

- 1 Connect the laptop to port 39 or 40 of the switch of the Dell Hybrid Cloud System for Microsoft stamp. This switch is the network switch that you use for management of Dell Hybrid Cloud System for Microsoft infrastructure components through iDRAC connections.
- 2 Configure the laptop with a static IP address from the iDRAC subnet range. This step enables network communication to the iDRACs in the Dell Hybrid Cloud System for Microsoft stamp.
- 3 Install Java version 7—or a later version—on this laptop so that you can start the virtual console through the iDRAC interface.

Ensure AD DS services are available.

Ensure that your Active Directory Domain Services (AD DS) infrastructure is available and functional.

Step 1: Verify that the storage is available and functional

- 1 If the iDRACs are connected, Dell recommends that you use a laptop. Configure the laptop and connect it to port 39 or 40 of the switch, then complete the following steps.
- 2 From the laptop, connect to the IPv4 iDRAC address of one of the file server cluster hosts by using a browser, for example, open <https://192.168.164.131>.
- 3 Ping the file server cluster hosts until they respond. It may take 10-20 minutes for them to be reachable. When the file server cluster hosts start to respond, do the following:
 - a To connect to one of the hosts and start a virtual console, use the iDRAC.
 - b Log on with an account that is a member of the **<Prefix>-Setup-Admins** group.
 - c Start a Windows PowerShell session, and then run the following commands:
 - 1 **Get-StorageEnclosure** to verify that all enclosures are up.
 - 2 **Get-ClusterSharedVolume** to verify that all CSVs are online.
 - 3 **\$p = Get-PhysicalDisk** followed by **\$p.count** . This should return 50, which is the number of physical disks on each rack (40 HDDs, 8 SSDs, 2 local drives).
 - 4 **Get-StoragePool** to verify that the pool has been discovered and find out its health state.
 - 5 **Get-VirtualDisk** to verify whether all the spaces are online.

After you verify that the storage is running and healthy, continue to the next procedure.

Step 2: Ensure that the IPv4 cluster core resources are online

- 1 Use Remote Desktop Connection to connect to the Console VM with an account that is a member of the **<Prefix>-Setup-Admins** group.
- 2 Open Failover Cluster Manager.
- 3 Connect to the storage cluster.
- 4 Click the storage cluster name, and then, in the **Cluster Core Resources** pane, expand the server name.
- 5 If the IPv4 Address resources have a status of **Offline**, right-click each of them, and then click **Bring Online**.
- 6 In Failover Cluster Manager, connect to the compute cluster.
- 7 Click the compute cluster name, and then, in the **Cluster Core Resources** pane, expand the server name.
- 8 If the IPv4 Address resources have a status of **Offline**, right-click each of them, and then click **Bring Online**.

If you cannot connect to the compute cluster by using Failover Cluster Manager, you can alternatively do the following:

- a Open Windows PowerShell.
- b Run the following command to check if the Cluster IP resources are online:
Get-ClusterResource -Cluster <ClusterName> | where {\$_.Name -like "Cluster IP Address*"}
- c Run the following command to get the exact name of the cluster IP resources:
Get-ClusterResource -Cluster <ClusterName> | where {\$_.Name -like "Cluster IP Address*" } | Format-List -Property Name
- d Start the IP address resource:
Start-ClusterResource "<IP ClusterResourceName>"

Repeat steps 2 through 4 for each IPv4 address cluster resource for the compute cluster and storage cluster where these resources are offline.

Step 3: Ensure the Windows Azure Pack services are running

Because in this scenario there is no control over the order of the components coming up, Dell recommends that you restart the infrastructure VM named **<Prefix>APA01**. To do this, follow the steps below.

- 1 Use Remote Desktop Connection to connect to the Console VM with an account that is a member of the **<Prefix>-Setup-Admins** group.
- 2 Open Failover Cluster Manager.
- 3 Connect to the compute cluster.
- 4 Click **Roles**, and then restart the **<Prefix>APA01** VM.

Step 4: Ensure that the Windows Azure Pack portals are working

The Windows Azure Pack portals depend on a security token service such as AD FS or an external third-party identity system for your domain.

Make sure that you can access the Windows Azure Pack management and tenant portals.

Step 5: Ensure that the backup infrastructure is up and running

If the iDRACs are connected, Dell recommends that you use a laptop, configured as described earlier in [Preparing your laptop](#).

- 1 From the laptop, connect to the IPv4 iDRAC address of one of the backup hosts by using a browser, for example, open `https://192.168.164.150`.
- 2 For each of the backup hosts, do the following:
 - a To connect to the host and open a virtual console, use the iDRAC.
 - b Log on with an account that is a member of the **<Prefix>-Setup-Admins** group.
 - c To verify that all the disks are online, run the Windows PowerShell cmdlet **Get-Disk**, for example:

```
[s20b01]: PS C:\> Get-Disk
```

Number	Friendly Name	OperationalStatus
2	Microsoft Virtual Disk	Online
0	DELL PERC H730P Mini SCSI Disk Device	Online
1	DELL PERC H730P Mini SCSI Disk Device	Online
 - d To verify that all the volumes are healthy, run the **Get-Volume** cmdlet. You should see nine volumes with a drive letter and one volume without a drive letter. Ensure that all are in healthy state, for example:

```
[s20b01]: PS C:\> Get-Volume
```

DriveLetter	FileSystemLabel	FileSystem	DriveType	HealthStatus
D		NTFS	Fixed	Healthy
H	Scratch	NTFS	Fixed	Healthy
I	Backup-S20DPM01-1	NTFS	Fixed	Healthy
J	Backup-S20DPM01-2	NTFS	Fixed	Healthy

K	Backup-S20DPM01-3	NTFS	Fixed	Healthy
L	Backup-S20DPM02-1	NTFS	Fixed	Healthy
M	Backup-S20DPM02-2	NTFS	Fixed	Healthy
N	Backup-S20DPM02-3	NTFS	Fixed	Healthy
C		NTFS	Fixed	Healthy
		NTFS	Fixed	Healthy

- e In the VMM console (in the **VMs and Services** workspace) or in Hyper-V Manager, check to make sure the DPM VMs that are hosted on this server are running.
- f Log on to each DPM VM, and verify the following:
 - 1 Open Disk Management (`Diskmgmt.msc`), and verify that there are 23 disks present, and that all are online. Disk numbering starts at Disk 0.
 - 2 Open the DPM Administrator console, open the **Management** workspace, and multiselect all the hosts. In the **Agents** group on the ribbon, click **Refresh**.
 - 3 In the protected computers, make sure that the agent status of all computers is **OK**.

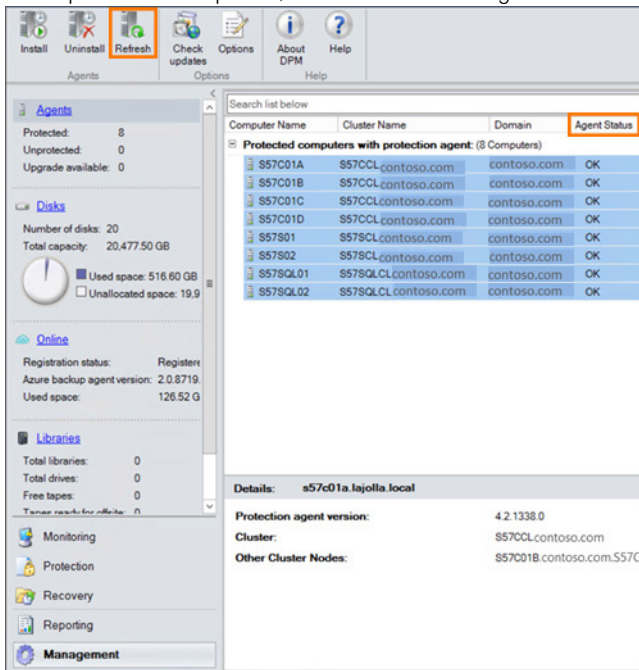


Figure 50. DPM Refresh Agent Status

- 4 In the navigation pane, click **Disks**, and verify that the DPM storage pool has 20 disks. Look for **DPM Storage Pool Disks (Total: 20)** in the heading, and that the status of all disks is green (checkmark).
- 5 If you opted in to Azure Backup, in the navigation pane, click **Online**, and make sure that the online status is green (checkmark).

After you verify that the backup infrastructure is working correctly, continue to the next procedure.

Step 6: Clear Operations Manager alerts generated during startup

- 1 Connect to the **<Prefix>CON01** VM with an account that is a member of the **<Prefix>-Ops-Admins** group.
- 2 Open the Operations Manager Shell.

- 3 Clear all rule-based alerts that Operations Manager generated during startup by running the following commands:

```
$InstanceObject = Get-SCOMClass -Name Microsoft.SystemCenter.ManagementServersGroup  
| Get-SCOMClassInstance | Get-SCOMMonitoringObject  
  
Start-SCOMTask -Task (Get-SCOMTask -Name Microsoft.Cloud.Overrides.Tasks.ResolveAlertsPerMP)  
-Instance $InstanceObject
```

Step 7: Verify the health of the Dell Hybrid Cloud System for Microsoft components

- 1 On the Console VM, open the Operations console.
- 2 In the **Monitoring** workspace, expand **Microsoft Cloud Dashboard**, and then click **Microsoft Cloud Dashboard**.
- 3 Make sure all components are healthy.

Security

This chapter discusses security issues pertaining to:

- User accounts
- Passwords
- Encryption keys
- Managing antivirus, antimalware, and certificates.

Topics:

- [User accounts and groups that are added by default](#)
- [Resetting service account passwords](#)
- [Rotating Windows Azure Pack encryption keys](#)
- [Managing antivirus and antimalware](#)
- [Managing certificates](#)

User accounts and groups that are added by default

Tables in this section identify and describe user accounts and security groups that are created by the Dell Hybrid Cloud System for Microsoft deployment process.

All Active Directory objects for Dell Hybrid Cloud System for Microsoft are created in the Active Directory organizational unit (OU) that you specified during deployment.

NOTE: Never log on to Dell Hybrid Cloud System for Microsoft, or sign in to the Windows Azure Pack website, by using service accounts. Do not use service accounts directly for administrative operations. Service accounts should only be used by Dell Hybrid Cloud System for Microsoft services and processes to communicate internally.

User accounts

Because the Dell Hybrid Cloud System for Microsoft is integrated with your Active Directory domain, you can use existing domain user accounts for management. Make sure you add accounts to the appropriate security groups. See the [Groups](#) table as well.

Table 33. User accounts

Type	Accounts	Privileges	Usage	Password Management
Delegated administrator	Account is specified by customer during deployment.	Has Full Control permissions to the parent OU (and all child objects) that was created for the Dell Hybrid Cloud System for Microsoft in Active	Used to deploy the Dell Hybrid Cloud System for Microsoft stamp.	Controlled via domain policy.

Type	Accounts	Privileges	Usage	Password Management
		Directory Domain Services.		
Dell Managed Accounts	iDRAC	Account administrator	Out-of-band management	Default password: p@ssw0rd Password rotation: Manual

Service accounts

This section discusses:

- Local service accounts
- Domain service accounts.

Local service accounts

The local service accounts that are required for Windows Azure Pack are listed in the following table.

Table 34. Local service accounts

Account	Account Type	Privileges/Usage
MonitoringClient	Local user	WAP to talk to Monitoring Service.
WebAppGalleryClient	Local user	WAP to talk to WAG service.
UsageAdminAPIClient	Local user	WAP to talk to Usage.
Spfuser (on APA01)	Local user	WAP to talk to SPF. Not owned by WAP.
SMAUser (on APA01)	Local user	WAP to talk to SMA. Not owned by WAP.

The following are the Windows Azure Pack service runtime accounts that are used for SQL Auth Connection strings. They are all SQL Server logins on <Prefix>SQLIN01\SQLIN01.

- AdminSiteNotificationServiceUser
- AuthSiteNotificationServiceUser
- MgmtSvc-AdminAPI
- MgmtSvc-AdminSite
- MgmtSvc-AuthSite
- MgmtSvc-Monitoring
- MgmtSvc-TenantAPI
- MgmtSvc-TenantPublicAPI
- MgmtSvc-TenantSite
- MgmtSvc-Usage
- MgmtSvc-UsageCollector

- MgmtSvc-UsageCollector_Management
- MgmtSvc-WebAppGallery
- MgmtSvc-WindowsAuthSite
- TenantSiteNotificationServiceUser

You do not have to touch any of these accounts. For all these accounts:

- The passwords are autogenerated.
- Password rotation is done when you run the MCPasswordReset script.

The password expiration for SpfUser and SMAUser is controlled by domain policy. All Windows Azure Pack database account passwords do not expire. However, they are rotated on the same schedule.

NOTE: Password policies are located in the following location in the Group Policy Management Console: **Default Domain Policy/Computer Configuration/Policies/Windows Settings/Security Settings/Account Policies/Password Policy**. For more information about security considerations of editing password policy settings, see [Domain Level Account Policies](#) on Microsoft TechNet.

Domain service accounts

The domain service accounts that are part of Dell Hybrid Cloud System for Microsoft are listed in the following table.

You do not have to touch any of these accounts. The following statements apply for all domain service accounts except for the <Prefix>SA-SMA and <Prefix>Installer accounts:

- The passwords are auto generated.
- Password rotation is done when you run the MCPasswordReset script.
- Password expiration is controlled via the domain policy.

NOTE: The password for the SMA group Managed Service Account, <Prefix>-SA-SMA, is autogenerated and automatically rotated by Active Directory Domain Services every two days. This password is not rotated by the MCPasswordReset script.

Table 35. Domain service accounts

Account	Privileges/Usage
<Prefix>-Installer	Used during deployment. By default, this account is disabled after deployment. This password is not rotated by the MCPasswordReset script NOTE: Do not remove or manually enable this account. This account is used during stamp expansion and backup deployment scenarios, where it is automatically enabled and then disabled again.
<Prefix>-Fabric	Administrator on physical hosts. Used for host management operations. For example, physical computers are added into VMM by using this account.
<Prefix>-System	Administrator on all management VMs. Used to communicate between VMs to run role operations, for example, to run runbooks, agent installation, and updates.
<Prefix>-SVC-SQL	Administrator on SQL VMs. Also has Read/Write permission for ServiceAccountPrincipal to do SPN registration. Used to run SQL Server services.
<Prefix>-SVC-VMM	Administrator on the VMM VM. Used to run the VMM service.
<Prefix>-SVC-OM	Administrator on the Operations Manager VM. Used to carry out actions on monitored computers across a network connection.
<Prefix>-SVC-SPF	Used to run all SPF services.

Account	Privileges/Usage
<Prefix>-SVC-SMA	Account used to deploy SMA.
<Prefix>-SA-SMA	Used to run all SMA services—SMA Web Service and SMA Runbook Service. This is a group Managed Service Account, called a gMSA account.

Groups

The following table describes security groups created by the Dell Hybrid Cloud System for Microsoft deployment process.

Table 36. Security groups

Group Name	Scope	Usage	Details
<Prefix>-Ops-Admin	Domain Local	<p>To provide administrators with access for day-to-day management operations.</p> <p>Users and groups can be added to this group from trusted domains.</p>	<ul style="list-style-type: none"> Local administrator on all infrastructure VMs. Has administrator rights to VMM, Operations Manager, DPM, and the Windows Azure Pack management portal for administrators.
<Prefix>-Diag-Admin	Domain Local	<p>Provides administrators with user rights to perform operations that require access to physical hosts and to management SQL Server databases.</p> <p>Users and groups can be added to this group from trusted domains.</p>	<ul style="list-style-type: none"> This group is a member of <Prefix>-Ops-Admins. Member of the sysadmin role in SQL Server. Member of the local Administrators group on all physical nodes.
<Prefix>-Setup-Admins	Global	<p>Provides administrators with elevated user rights to perform operations such as patching and updating of Dell Hybrid Cloud System for Microsoft, and password reset.</p> <p>Users and groups can be added from the domain in which the Dell Hybrid Cloud System for Microsoft stamp is a member.</p>	<p>This group is a member of <Prefix>-Diag-Admins. Has elevated permissions within the Dell Hybrid Cloud System for Microsoft OU. For example, a member of this group can run MCPasswordReset to reset service account passwords for components in the OU.</p> <p>Dell recommends that you add users to this group only for specific, setup-related operations, and that you revoke access to added users when setup operations are finished.</p>
<Prefix>-SMA-VMs	Global	<p>Do not add or remove accounts from this group.</p>	<p>This is a security group that is needed to assign access to the group Managed Service Account (gMSA account) for SMA. The SMA VM computer account is a member of this group.</p>

Resetting service account passwords

This section describes how to rotate service account passwords by using the password reset script. It is important that you do this rotation *before* service account passwords expire. Password expiration is controlled by your domain password policy settings. The Operations Manager alert for password expiration is raised 14 days before passwords expire.

IMPORTANT: If service account passwords have already expired, complete the steps in the following section before you run the password script.

Resetting expired service account passwords

Use the following instructions to reset and resynchronize your expired DHCS service account passwords with the Active Directory environment. These instructions also help you restore full functionality to all the services that may be impacted after all account passwords have expired. When expiration occurs, you might find that the SQL instances within the SQL cluster cannot start, and services that rely on those instances, such as SCVMM, SCOM, and Azure, do not function properly. Follow these steps to restore functionality:

- 1 Find accounts that have expired, using the following command:

```
Get-ADUser -filter {Enabled -eq $True -and PasswordNeverExpires -eq $False}-Properties "Name", "msDS-UserPasswordExpiryTimeComputed" | Select-Object -Property "Name", @{Name="ExpiryDate";Expression={[datetime]::FromFileTime($_.msDS-UserPasswordExpiryTimeComputed)}}
```

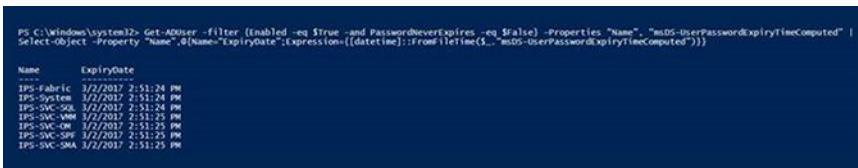


Figure 51. Find expired accounts

- 2 Reset SQL service account password by doing the following:
 - a Launch **Active Directory Users and Computers**, and locate the SQL service account, **<Prefix>-SVC-SQL**.
 - b Right-click and select **Reset Password** to open a dialog where you can type a new password. Deselect **User must change password at next logon** before clicking **OK**.



Figure 52. Reset Password dialog

- c Open the Services console (**services.msc**), and connect to the first SQL cluster node, **<Prefix>SQL01**.
- d Locate the SQL Instance services:

- SQL Server (SQLIN01)
- SQL Server (SQLIN02)
- SQL Server Agent (SQLIN01)
- SQL Server Agent (SQLIN02)

SQL Server (SQLIN01)	Provides sto...	Running	Manual	SYSMGMT\IPS-SVC-SQL
SQL Server (SQLIN02)	Provides sto...		Manual	SYSMGMT\IPS-SVC-SQL
SQL Server Agent (SQLIN01)	Executes jo...	Running	Manual	SYSMGMT\IPS-SVC-SQL
SQL Server Agent (SQLIN02)	Executes jo...		Manual	SYSMGMT\IPS-SVC-SQL

Figure 53. SQL instances

- Open the properties for each service, select the **Log On** tab, change the password, and click **OK**.
 - Once the password has been changed for each service, open **Failover Cluster Manager**, and then connect to the SQL cluster, **<Prefix>SQLCL**.
 - Select **Nodes**, right-click on the first node, **<Prefix>SQL01**, and select **Pause > Drain Roles**.
 - Restart the node, and once it is back in a paused state you can proceed to right-click on the node, and select **Resume > Fail Roles Back**.
 - Continue with the next node, **<Prefix>SQL01**, from step c onward.
- Reset the VMM service account password, as follows:
 - Launch **Active Directory Users and Computers**, and locate the SQL service account, **<Prefix>-SVC-VMM**.
 - Right-click and select **Reset Password** to open a dialog where you can type a new password. Deselect **User must change password at next logon** before clicking **OK**.
 - Open the Services console (**services.msc**), and connect to the VMM server, **<Prefix>VMM01**.
 - Locate the System Center Virtual Machine Manager service.

Spot Verifier	Verifies pot...		Manual (Trig...	Local System
Storage Tiers Management	Optimizes t...		Manual	Local System
System Center Virtual Machine Manager	Provides ser...		Automatic	SYSMGMT\IPS-SVC-VMM
System Center Virtual Machine Manager Agent	Provides m...	Running	Automatic	Local System
System Event Notification Service	Monitors sy...	Running	Automatic	Local System

Figure 54. System Center Virtual Machine Manager service

- Open the properties for the service, select the **Log On** tab where you can change the password, and then click **OK**.
 - Right-click once more, and select **Start** to start the VMM service.
- Reset the System account password in Active Directory, Service Management Automation (SMA), and VMM by doing the following:
 - Launch **Active Directory Users and Computers**, and locate the System service account, **<Prefix>-System**.
 - Right-click and select **Reset Password** to open a dialog where you can type a new password. Deselect **User must change password at next logon** before clicking **OK**.
 - Next, run the **Set-SmaCredential** cmdlet to set the matching password in SMA.


```
Set-SmaCredential -Name "<Prefix>-System" -Value (Get-Credential) -WebServiceEndpoint https://<endpoint>
```

For example, where **<Prefix>** equals IPS, and **<endpoint>** equals **<Prefix>APA01**, the command is as follows:

```
Set-SmaCredential -Name "IPS-System" -Value (Get-Credential) -WebServiceEndpoint https://IPSAPA01
```
 - When prompted for credentials, enter the System service account username, and enter the password that you used in step b.
 - Next, open the VMM management console, and connect to the VMM server, **<Prefix>VMM01**.
 - In the **Settings** workspace, expand **Security**, and then select **Run As Accounts**.

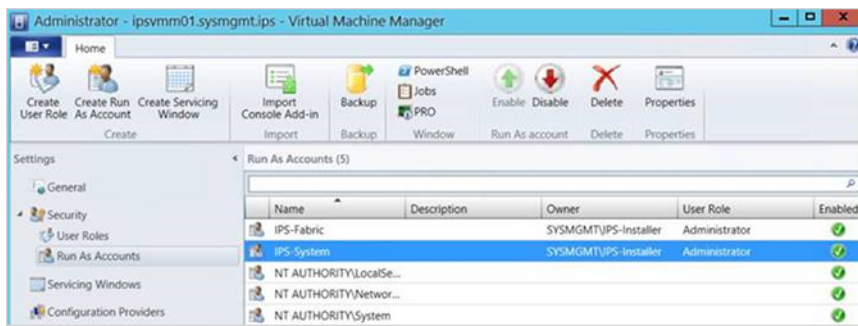


Figure 55. List of the Run As accounts

- g Right-click the **CPS-System** Run As account, and then click **Properties**.
 - h Type the same password that you set in **Active Directory Users and Computers** in step b, and then click **OK**.
- 5 Reset the **Fabric** account password in both Active Directory and VMM as follows:
- a Launch **Active Directory Users and Computers**, and locate the System service account, **<Prefix>-Fabric**.
 - b Right-click and select **Reset Password** to open a dialog where you can type a new password. Deselect **User must change password at next logon** before clicking **OK**.
 - c Open the VMM management console, and connect to VMM server, **<Prefix>VMM01**.
 - d In the **Settings** workspace, expand **Security**, and then select **Run As Accounts**.

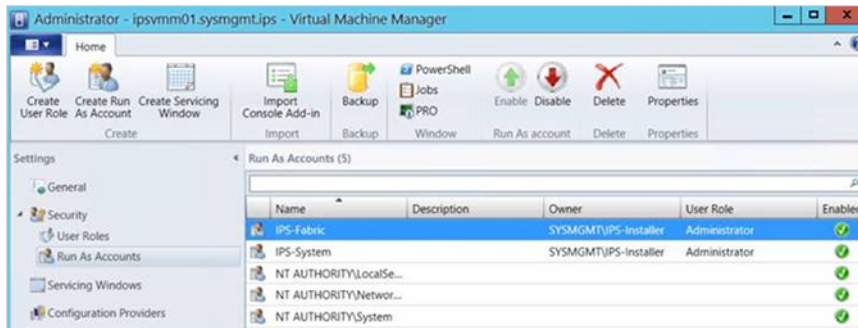


Figure 56. List of the Run As accounts

- e Right-click the **CPS-Fabric** Run As account, and then click **Properties**.
- f Type the same password that you set in **Active Directory Users and Computers** in step b, and then click **OK**.
- g To validate VMM functionality, select the **Fabric** workspace, expand **Servers > All Hosts**, right-click the compute cluster, **<Prefix>CCL**, and then click **Refresh**.



Figure 57. List of recent jobs

- h Verify that the refresh job completes. The message **Completed w/info** indicates success.
- 6 Reset the OM service account password in both Active Directory and SCOM, as follows:
- a Launch **Active Directory Users and Computers**, and locate the System service account, **<Prefix>-SVC-OM**.
 - b Right-click and select **Reset Password** to open a dialog where you can type a new password. Deselect **User must change password at next logon** before clicking **OK**.
 - c Open the services console (**services.msc**), and connect to the SCOM server, **<Prefix>OM01**
 - d Locate the SCOM services:
 - System Center Data Access Service

- System Center Management Configuration

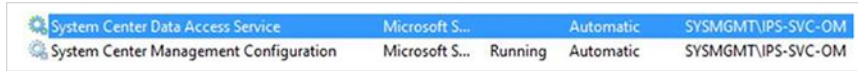


Figure 58. SCOM services

- Open the properties for each service, select the **Log On** tab, change the password to what was set in **Active Directory Users and Computers** in step b, and then click **OK**.
- Once the password has been set, right-click on each service, and select:
 - **Start** if not running
 - **Stop** then **Start** if previously running
- Next, open the SCOM management console, and connect to the SCOM server if prompted, **<Prefix>OM01**.
- Select the **Administration** workspace, and under the **Run As Configuration** menu option select **Accounts**.

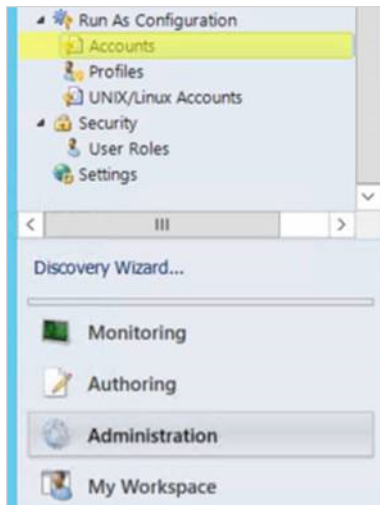


Figure 59. Select Accounts under Run As Configuration

- Double-click the SCOM action account, **<Prefix>-SVC-OM**, under the **Action Account** section to bring up the properties.

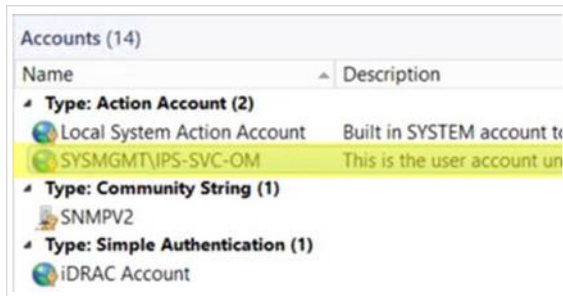


Figure 60. SCOM action accounts

- Select the **Credentials** tab, type the same password that you set in **Active Directory Users and Computers** in step b, and then click **OK**.
- Select the **Monitoring** workspace, click **Active Alerts** under the **Monitoring** section, and close out any active alerts that pertain to the Run As account not being able to log on.

Severity: Critical (20)					
✘	IPSS7.sysmgmt.Ips	Run As Account Could Not Log On	New	3/2/2017 11:25:04 P...	4 Days, 17 ...
✘	IPDOM01.sysmgmt.Ips	Run As Account Could Not Log On	New	3/2/2017 11:25:04 P...	4 Days, 17 ...
✘	IPSDPM02.sysmgmt.Ips	Run As Account Could Not Log On	New	3/2/2017 11:25:04 P...	4 Days, 17 ...
✘	IPSDPM01.sysmgmt.Ips	Run As Account Could Not Log On	New	3/2/2017 11:25:03 P...	4 Days, 17 ...
✘	IPSS5.sysmgmt.Ips	Run As Account Could Not Log On	New	3/2/2017 11:25:03 P...	4 Days, 17 ...
✘	IPSA01.sysmgmt.Ips	Run As Account Could Not Log On	New	3/2/2017 11:25:03 P...	4 Days, 17 ...
✘	IPSSQL02.sysmgmt.Ips	Run As Account Could Not Log On	New	3/2/2017 6:02:14 PM	4 Days, 23 ...
✘	IPSSQL01.sysmgmt.Ips	Run As Account Could Not Log On	New	3/2/2017 6:02:14 PM	4 Days, 23 ...

Figure 61. Monitoring workspace

- I To verify that the password change was successful, monitor for any new Run As account alerts.
- 7 Reset the SPF and SMA service accounts in Active Directory and local accounts on **<Prefix>APA01** as follows:
 - a Launch **Active Directory Users and Computers**, and locate the SPF and SMA service accounts, **<Prefix>-SVC-SPF** and **<Prefix>-SVC-SMA**.
 - b Right-click and select **Reset Password** to open a dialog where you can type a new password. Deselect **User must change password at next logon** before clicking **OK**.
 - c From an administrative PowerShell session, connect to **<Prefix>APA01** using the following command:

```
Enter-PSSession <PREFIX>APA01
```
 - d Change to the following directory:

```
cd 'C:\Program Files\Management Service\MgmtSvc-PowerShellAPI\Samples\Diagnostic'
```
 - e Execute the **Test-WapResourceProviderEndpoints.ps1** script to get the current passwords for the local spfuser and smauser:

```
.\Test-WapResourceProviderEndpoints.cmd
```

```
VERBOSE: ===== BEGIN Test-WapResourceProvider systemcenter
VERBOSE: {
  "Name": "systemcenter",
  "InstanceId": "CA4C41CC-85C8-472C-A6D1-669BF2EA9967",
  "DisplayName": "Virtual Machine Clouds",
  "AdminForwardingAddress": "https://ipsapa01.sysmgmt.ips:8090/",
  "AdminUsername": "spfuser",
  "AdminPassword": "GQ2kcGoF@aSRTCHU"
}
```

Figure 62. Example output for spfuser

```
VERBOSE: ===== BEGIN Test-WapResourceProvider automation
VERBOSE: {
  "Name": "automation",
  "InstanceId": "7B4D305C-FF4E-43FC-ABE0-E4958AF51B9C",
  "DisplayName": "Automation",
  "AdminForwardingAddress": "https://ipsapa01.sysmgmt.ips:9090/",
  "AdminUsername": "smauser",
  "AdminPassword": "WcoIztY6RsmQGEGG"
}
```

Figure 63. Example output for smauser

- f Open **Computer Management** from the **Tools** menu in **Server Manager**.
- g Connect to the **<Prefix>APA01** server.
- h Expand **System Tools > Local Users and Computers**, and then select **Users**.

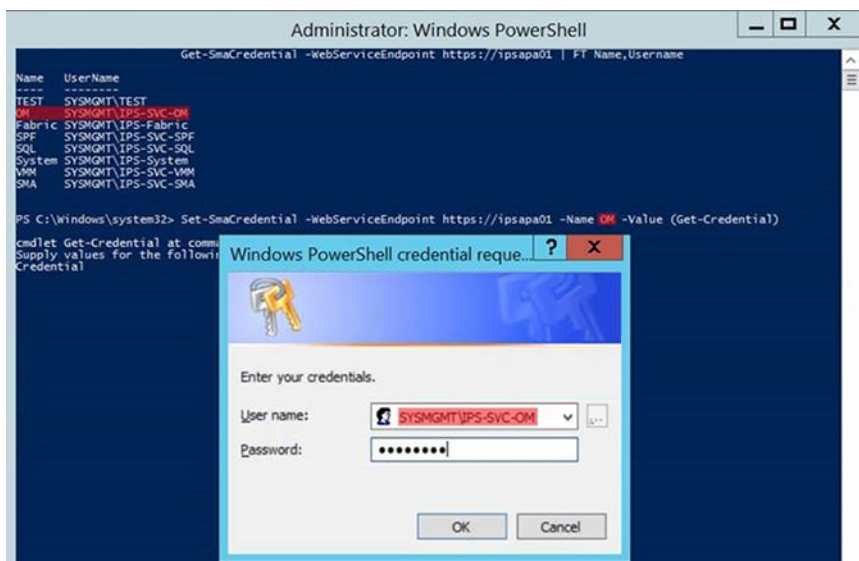
- i Right-click the **smauser**, select **Set Password**, and click **Proceed** when prompted.
 - j Enter the password that was output by the **Test-WapResourceProviderEndpoints.ps1** script, and click **OK**.
 - k Right-click the **spfuser**, select **Set Password**, and click **Proceed** when prompted.
 - l Enter the password that was output by the **Test-WapResourceProviderEndpoints.ps1** script, and click **OK**.
 - m Confirm that the passwords work by opening the Admin portal.
- 8 Reset the SMA stored service accounts passwords on **<Prefix>APA01** as follows:
- a From an administrative PowerShell session, get a list of the current stored SMA credentials:

```
PS C:\Windows\system32> Get-SmaCredential -WebServiceEndpoint https://ipsapa01 | FT Name,Username

Name      UserName
----      -
OM        SYSMGMT\IPS-SVC-OM
Fabric    SYSMGMT\IPS-Fabric
SPF       SYSMGMT\IPS-SVC-SPF
SQL       SYSMGMT\IPS-SVC-SQL
System    SYSMGMT\IPS-System
VMM       SYSMGMT\IPS-SVC-VMM
SMA       SYSMGMT\IPS-SVC-SMA
```

Figure 64. Example output for SmaCredential

- b Set each SMA credential that contains the solution prefix with the following code block. Utilize the name from the previous step's output with the **Get-Credential** cmdlet to set the username and password.
- ```
Set-SmaCredential -WebServiceEndPoint https://<PREFIX>apa01 -Name <NAME> -Value (Get-Credential)
```
- c When prompted for the username and password, enter the username in **domain\username** form and the password of the service account you are configuring.



**Figure 65. Windows PowerShell credential request**

**NOTE:** The Operations Manager Service Account in the output at the top of the graphic provides the **-Name** value **OM** which is used to set the credential. In the dialog, enter the user name in **domain\username** format, and then type your domain password.

- d Perform the above steps on each of the SMA credentials found that contain the solution prefix.

Once you have reset all the passwords, you can execute the **MCPasswordReset.ps1** script, and monitor for any additional errors. For instructions, see [How to run the MCPasswordReset script](#).

# How service accounts are managed

Dell Hybrid Cloud System for Microsoft includes a password reset script that you can use to change passwords for the following service accounts:

- <Prefix>-Fabric
- <Prefix>-System
- <Prefix>-SVC-SQL
- <Prefix>-SVC-VMM
- <Prefix>-SVC-OM
- <Prefix>-SVC-SPF
- <Prefix>-SVC-SMA

It is recommended that you run the **MCPasswordReset** script to reset the passwords for these service accounts whenever you are alerted to do so by System Center Operations Manager. These accounts are described in [User accounts and groups that are added by default](#).

## ❗ **IMPORTANT: Read this entire section before you run the script.**

Starting with the Microsoft update version 1603A, the Operations Manager alert for password expiration is raised 14 days before passwords expire, rather than three days as in previous releases. To view remaining time before the next password expiration without waiting for an alert, run the following command in Windows PowerShell on the Console VM:

```
Get-ADUser -filter {Enabled -eq $True -and PasswordNeverExpires -eq $False} -Properties "DisplayName", "msDS-UserPasswordExpiryTimeComputed" | Select-Object -Property "SAMAccountName", @{Name="ExpiryDate";Expression={ [datetime]::FromFileTime($_."msDS-UserPasswordExpiryTimeComputed") }}
```

For each account, the **MCPasswordReset** script does the following:

- Automatically generates a new password.
- Updates the credentials that are stored in SMA with the new password.
- Changes the password for each account in AD DS.
- Each runbook that is run by the **MCPasswordReset** script also updates the passwords in related management components. This includes the Windows services and the Run As accounts, and all local passwords that are required by the Windows Azure Pack portals for administrators and tenants.

## Important information about the password reset script

Keep the following points in mind about the **MCPasswordReset** script:

- The **MCPasswordReset** script is fairly disruptive. It restarts many services, and results in some downtime of management infrastructure components. Consider running it within a planned maintenance window.
- The **MCPasswordReset** script works when all Dell Hybrid Cloud System for Microsoft infrastructure VMs and services are running normally (that is, not in maintenance mode), and Dell Hybrid Cloud System for Microsoft service account passwords described at the start of this section are not expired and are in sync. Recovering from a condition when one or more Dell Hybrid Cloud System for Microsoft service account passwords are expired is not the purpose of this script.
- Operations Manager sends the following alert to customers when passwords are about to expire.

**Alert Name:** Run As Account(s) Expiring Soon

**Alert Description:** One or more Run As account passwords are expiring soon. Update the passwords for Run As accounts to prevent problems with monitoring. To update your Run As account passwords, please update the passwords using the procedures described in the [How service accounts are managed](#) section of the Administrators Guide.



- You must be a member of the **<Prefix>-Setup-Admins** group in the Dell Hybrid Cloud System for Microsoft OU to run the **MCPasswordReset** script. You are prompted to provide those credentials when you run the script.
- The password reset script works only for the accounts listed in the preceding section. It does not reset passwords for any manually-created accounts, or for Windows Azure Pack encryption keys.
- Run only the **MCPasswordReset** script. Do not run the **Reset-\*Password** runbooks that support the script. The supporting runbooks are invoked automatically by the **MCPasswordReset** script, and are not to be run individually.
- Interrupting the **MCPasswordReset** script requires manual recovery. Avoid interrupting the password reset process.

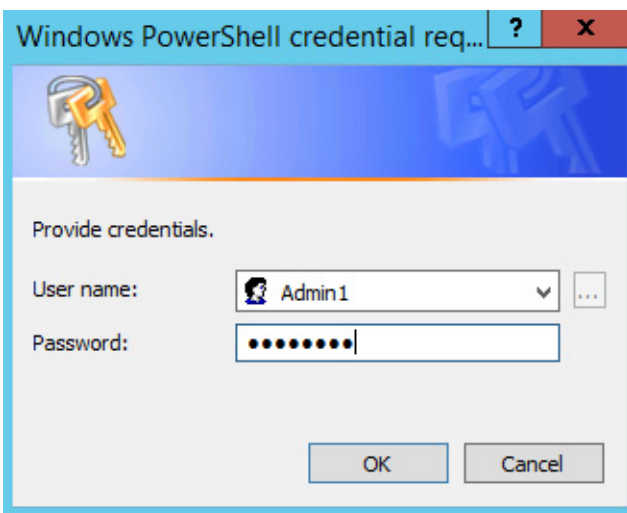
## How to run the MCPasswordReset script

Do the following:

- 1 Log on to the Console VM.
- 2 Open an elevated Windows PowerShell session.
- 3 Change directories to **C:\Program Files\Microsoft Cloud Solutions\PasswordReset**.  
For example: **PS C:\Users> cd C:\Program Files\Microsoft Cloud Solutions\PasswordReset**.
- 4 Type the following command to start the script, and then press **Enter**:  
**.\MCPasswordReset.ps1**

For example, **PS C:\Program Files\Microsoft Cloud Solutions\PasswordReset> .\MCPasswordReset.ps1**.

- 5 You are prompted to provide **<Prefix>-Setup-Admins** credentials. Specify the user name and password. You do not have to provide the domain. For example, specify a user name of **Admin1**, as shown in the following screenshot. Do not specify **Domain\Admin1**.



**Figure 66. Admin login**

- 6 The script displays progress while it runs. Do not close the Windows PowerShell session or try to interrupt the script while it is running. If you interrupt the script, this can put the components in an inconsistent state. The script typically requires 12 to 15 minutes to finish. The following screenshot is an example of the report that is displayed when the script finishes. If the **Status** of any of the runbooks is **Failed** or **Failed to complete**, see [Troubleshooting the MCPasswordReset script](#). To view **MCPasswordReset** log files, see [Viewing MCPasswordReset script logs](#).

```

2015-09-01 14:44:25 Info: Runbook Reset-SpfPassword completed
2015-09-01 14:44:28 Info: Password reset finished. Uploading log.
2015-09-01 14:44:29 Info:
Runbook Status

Reset-SQLPassword Completed
Reset-VmmServiceAccountPassword Completed
Reset-VmmPassword Completed
Reset-Ormpassword Completed
Reset-MgmtSvcCorePassword Completed
Reset-MgmtSvcPublicPassword Completed
Reset-SmaPassword Completed
Reset-SpfPassword Completed

2015-09-01 14:44:29 Info: Runbook PasswordReset-Log started
2015-09-01 14:44:29 Info: Runbook job ID: 91bd8f19-772d-422b-b06b-3d85afcefa13
2015-09-01 14:44:40 Info: Runbook PasswordReset-Log completed
PS C:\Program Files\Microsoft Cloud Solutions\PasswordReset>

```

Figure 67. MCPasswordReset report

These are the tasks performed by the `MCPasswordReset` script, in order:

- 1 The script verifies that the following required Dell Hybrid Cloud System for Microsoft components are available and running normally. If these components are not running, the script stops:
  - SMA server
  - SMA database
- 2 The script performs a basic health check on components it must access to change passwords. Specifically, the script verifies that all VMs, related services, and SQL Server instances are running.
- 3 If step 2 is successful, the script resets the passwords described at the start of this section.

If required VMs or services are not running, the script prompts you with the following warning:

**Some virtual machines or services are not running. Do you want to continue?**

It is recommended that you type `N`, and then press **Enter** to stop the script. It is preferable that you do not continue because more failures can occur during the password reset process.

If step 2 fails, the script displays a list of required VMs and services and their states, for troubleshooting purposes.

## Viewing MCPasswordReset script logs

To help troubleshoot issues with the `MCPasswordReset` script, view the log files after you run the script.

### Viewing the log files using File Explorer

To get the log files using File Explorer, do the following:

- 1 On the Console VM, open File Explorer, and then open the folder `C:\Program Files\Microsoft Cloud Solutions\PasswordReset`.
- 2 A new folder with the following name convention is created each time you run the script: **PasswordReset\_YYYY-MM-DD\_HH-MM-SS**. Open this folder, and then open the file named **PasswordReset.log** to find a summary of script tasks.
- 3 The script's supporting runbook logs are also stored in the date- and time-stamped folder, for easier troubleshooting if individual runbook failures occur.

### Viewing the log files from SMA

Alternatively, you can get password reset script log files from SMA:

- 1 Log on to the VM that is running SMA (`<Prefix>APA01`) with any account that is a member of the `<Prefix>-Ops-Admins` group.

**NOTE:** You can also run the commands from the Console VM. However, if you do this, you must replace *localhost* in each of the following steps with the host name of the SMA VM.

- 2 In a Windows PowerShell console that is running with elevated user rights (Run as Administrator), run the **Get-SmaJob** cmdlet to find the job ID and the number of errors.

```
Get-SmaJob -RunbookName PasswordReset-Log -WebServiceEndpoint 'https://localhost'
```

- 3 Copy the job ID from the results of the **Get-SmaJob** command, and use it in the following commands.

- 4 Run the following commands to get the job output, specifying the job ID value that you obtained in step 3.

```
Get-SmaJobOutput -JobId JobId -Stream Error -WebServiceEndpoint 'https://localhost'
| %{ $_ } | sort StreamTime > Error.txt
```

```
Get-SmaJobOutput -JobId JobId -Stream Any -WebServiceEndpoint 'https://localhost'
| %{ $_ } | sort StreamTime > Any.txt
```

## Viewing job status and errors in the Windows Azure Pack portal

You can also view password reset script job status and errors in the Windows Azure Pack management portal for administrators as follows:

- 1 In the Windows Azure Pack management portal for administrators, click **Automation**.
- 2 Click **Runbooks**.
- 3 In the search text box, type the word `password`, and then click **Search**.
- 4 In the search results, click **PasswordReset-Log**.
- 5 Click **Jobs**. On the **Jobs** page, you can view the status of current jobs.
- 6 To view logs, select the most recent job.
- 7 To view only errors, click **History**, type `error` in the search text box, and then click **Search**.

## Troubleshooting the MCPasswordReset script

The following sections discuss two errors you may encounter when running the MCPasswordReset script, and how to resolve them.

### Error: Some virtual machines and/or services related to VMM, SMA, and/or SQL Server are not running

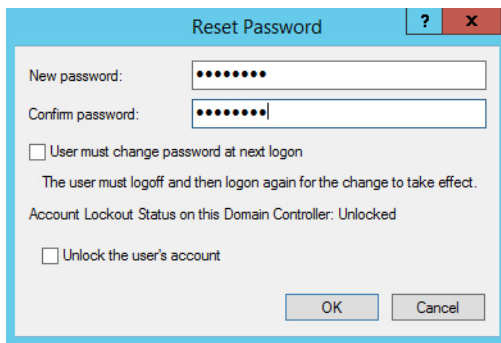
If you get the following error when you run the **MCPasswordReset** script, the service account passwords in VMM and/or SQL, or the `<Prefix>-System` account password in SMA might be out of sync with what is in AD DS. You must fix this issue manually for the **MCPasswordReset** script to run successfully.

#### ERROR

**Some virtual machines and/or services related to VMM, SMA, and/or SQL Server are not running. No passwords have been reset. For information about how to resolve this issue, see the [Troubleshooting the MCPassword Reset script](#) section of the Dell Hybrid Cloud System for Microsoft Administrators Guide.**

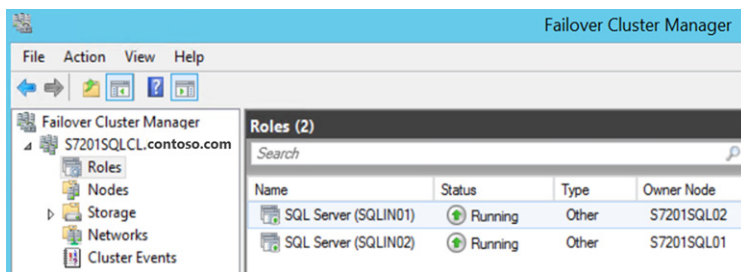
To synchronize SQL Server and VMM service account passwords:

- 1 **Step 1: Reset the password of the service accounts in AD DS.**
  - a Open **Active Directory Users and Computers** on a computer in your domain on which this is installed, as a user who has rights to do account management in AD DS.
  - b Expand the Dell Hybrid Cloud System for Microsoft **OU**, and then click the `<Prefix>-SVC-SQL` account.
  - c Right-click the account, and then click **Reset Password**.
  - d Change the password.
  - e Clear the check box for **User must change password at next logon**, and then click **OK**.



**Figure 68. Reset password**

- f Repeat this procedure for the **<Prefix>-SVC-VMM** account.
  - g Close **Active Directory Users and Computers**.
- 2 **Step 2: Reset the password of the service accounts in the Services snap-in.**
- a On the Console VM, open the **Failover Cluster Manager** console from the **Tools** menu in Server Manager.
  - b In the **Actions** pane, click **Connect to Cluster**. Select the **<Prefix>SQLCL** cluster. If the cluster is not listed in the drop-down list, click **Browse**. After you select the cluster, click **OK**.
  - c In the navigation pane, expand the cluster name, and then click **Roles**. In the **Owner Node** column, note the node on which the **SQLIN01** instance is running.



**Figure 69. SQL Server nodes**

- d Open the **Services** snap-in from the Server Manager **Tools** menu.
  - e In the **Services** snap-in, right click **Services (Local)**, and then click **Connect to another computer**.
  - f Type the name of the SQL Server guest cluster node on which SQLIN01 is **not** running.
  - g Perform this step for each of the following services:
    - **SQL Server (SQLIN01)**
    - **SQL Server Agent (SQLIN01)**
    - 1 Double-click the service to open the service's **Properties** dialog box, and then click the **Log On** tab.
    - 2 In the **Password** and **Confirm Password** boxes, type the password you set in AD DS for the **<Prefix>-SVC-SQL** account. Click **OK**, and then close the **Services** snap-in.
  - h Return to Failover Cluster Manager, and connect to the **<Prefix>SQLCL** cluster again, if you are still not connected.
  - i Click **Roles**, right-click the SQLIN01 instance, point to **Move**, and then click **Select Node**.
  - j Move the SQLIN01 instance to the node on which you changed passwords in step **g** of this procedure.
  - k In the **Services** snap-in, connect to the VMM virtual machine—**<Prefix>VMM01**.
  - l In the results pane, double-click the **System Center Virtual Machine Manager** service to open its **Properties** dialog box. Do the following:
    - 1 On the **Log On** tab, in the **Password** and **Confirm Password** fields, type the same password you provided for the **<Prefix>-SVC-VMM** account in AD DS. Click **OK**.
    - 2 Restart the service.
  - m Close the **Services** snap-in.
- 3 **Step 3: Synchronize the <Prefix> System account password in SMA, AD DS, and VMM**

If the <Prefix>-System password is not in synch between SMA, AD DS, and VMM, the **MCPasswordReset** script cannot run. To fix this:

- a Change the password for the <Prefix>-System account in **Active Directory Users and Computers**.
- b Run the **Set-SmaCredential** cmdlet to set the matching password in SMA. To do this, run the following commands from the VM that is running SMA—<Prefix>APA01:

```
$cred = Get-Credential
```

When you are prompted, enter <Domain>\<Prefix>-System, and the new password you set in **Active Directory Users and Computers**. Then, run the next line of the command.

```
Set-SmaCredential -Name "<Prefix>-System" -Value $cred -WebServiceEndpoint https://<Prefix>APA01.domain.com
```

- c Change the password of the <Prefix>-System Run As account in VMM:
  - 1 In the VMM console, open the **Settings** workspace.
  - 2 Expand **Security**, and then click **Run As Accounts**.
  - 3 Double-click <Prefix>-System.
  - 4 In the **Password** and **Confirm password** boxes, type the same password that you set in **Active Directory Users and Computers**, and then click **OK**.

## Error: Some virtual machines from VMM, SMA, and SQL Server are not running

The following error can occur when you try to run the **MCPasswordReset** script when required component VMs are not running.

### ERROR

**Some virtual machines from VMM, SMA, and SQL Server are not running. No passwords have been reset. For information about how to resolve this issue, see the [Troubleshooting the MCPasswordReset script](#) section of the Dell Hybrid Cloud System for Microsoft Administrators Guide. Virtual machines that are not running: <list of VMs not running>.**

This error can be caused by one of the following issues:

- The VMs shown in the error message are turned off. Verify that the VMs are turned on, and then try running the script again.
- One or more of the following account passwords is not in synch with AD DS:
  - VMM service account
  - SQL Server service account
  - <Prefix>-System account password in SMA
  - <Prefix>-Fabric Run As account password in VMM.

Out-of-synch passwords must be manually fixed for the **MCPasswordReset** script to run successfully.

To fix this issue, follow the procedures in [Error: Some virtual machines and/or services related to VMM, SMA, and/or SQL Server are not running](#), and then also complete the following procedure to synchronize the <Prefix>-Fabric account:

### To synchronize the <Prefix>-Fabric account password in both AD DS and VMM

If the <Prefix>-Fabric Run As account password in VMM is not in synch with AD DS, the **MCPasswordReset** script cannot run because it might not be able to get the state of required component VMs.

To fix this condition, do the following:

- 1 In **Active Directory Users and Computers**, expand the Dell Hybrid Cloud System for Microsoft OU, and then click the **<Prefix>-Fabric** account.
- 2 Right-click the account, and then click **Reset Password**.
- 3 Change the password.
- 4 Clear the check box for the **User must change password at next logon** option, and then click **OK**.
- 5 Close **Active Directory Users and Computers**.
- 6 Open the VMM console.
- 7 In the **Settings** workspace, expand **Security**, and then click **Run As Accounts**.
- 8 Right-click the **<Prefix>-Fabric** Run As account, and then click **Properties**.
- 9 Type the same password that you set in **Active Directory Users and Computers**. Click **OK**, and then close the VMM console.
- 10 Try running the **MCPasswordReset** script again.

## Rotating Windows Azure Pack encryption keys

Windows Azure Pack for Windows Server uses encryption algorithms, encryption keys, and passwords to secure communications between the databases and users in the management and tenant portals.

You can reset Windows Azure Pack account encryption keys if you believe they have been compromised or accessed by unauthorized users; or as part of periodic, regular security maintenance.

**NOTE:** Before you run Windows Azure Pack encryption key rotation runbooks, we strongly recommend that you back up the SQL Server databases, and all Windows Azure Pack VMs. For information about how to do this, see [Backup and recovery](#).

Use the following runbooks for password and encryption key rotation. You must run them in the listed order.

**Table 37. Runbooks for Encryption**

| Runbook Name                             | Description                                         | Order |
|------------------------------------------|-----------------------------------------------------|-------|
| <b>Reset-MgmtSvcCoreEncryption.ps1</b>   | Rotates encryption keys for sites on <Prefix>APA01. | 1     |
| <b>Reset-MgmtSvcPublicEncryption.ps1</b> | Rotates encryption keys for sites on <Prefix>APT01. | 2     |

To run the runbooks:

- 1 Sign in to the Windows Azure Pack management portal for administrators with an account that is a member of the **<Prefix>-Ops-Admins** group.
- 2 On the **Automation** page, click **Runbooks**.
- 3 Find and run the **Reset-MgmtSvcCoreEncryption** runbook.
- 4 Find and run the **Reset-MgmtSvcPublicEncryption** runbook.

## Managing antivirus and antimalware

The following sections discuss strategies for dealing with malware and virus threats.

### Overview of default antimalware configuration

During Dell Hybrid Cloud System for Microsoft deployment, Microsoft does the following:

- 1 Sets up VMM to install update baselines on managed servers.
- 2 Sets up Windows Server Update Services to automatically approve antimalware updates.



### 3 Installs System Center 2012 R2 Endpoint Protection.

The System Center Endpoint Protection management tools in the Operations Manager console display the computers that are protected. The following screenshot is an example:

| State   | Name                   | Antimalware Engine | Antimalware Activity | Antimalware Definitions |
|---------|------------------------|--------------------|----------------------|-------------------------|
| Healthy | S59VMM01.contoso.com   | Healthy            | Healthy              | Healthy                 |
| Healthy | S59SQLIN02.contoso.com | Healthy            | Healthy              | Healthy                 |
| Healthy | S59SQLIN01.contoso.com | Healthy            | Healthy              | Healthy                 |
| Healthy | S59SQLCL.contoso.com   | Healthy            | Healthy              | Healthy                 |
| Healthy | S59SQL02.contoso.com   | Healthy            | Healthy              | Healthy                 |
| Healthy | S59SQL01.contoso.com   | Healthy            | Healthy              | Healthy                 |
| Healthy | S59OM01.contoso.com    | Healthy            | Healthy              | Healthy                 |
| Healthy | S59CON01.contoso.com   | Healthy            | Healthy              | Healthy                 |
| Healthy | S59CCL.contoso.com     | Healthy            | Healthy              | Healthy                 |
| Healthy | S59CID.contoso.com     | Healthy            | Healthy              | Healthy                 |
| Healthy | S59C1C.contoso.com     | Healthy            | Healthy              | Healthy                 |
| Healthy | S59C1B.contoso.com     | Healthy            | Healthy              | Healthy                 |
| Healthy | S59C1A.contoso.com     | Healthy            | Healthy              | Healthy                 |
| Healthy | S59APT01.contoso.com   | Healthy            | Healthy              | Healthy                 |
| Healthy | S59APA01.contoso.com   | Healthy            | Healthy              | Healthy                 |

Figure 70. Endpoints with FEP

**NOTE:** If you click Endpoints without FEP, it is expected that storage nodes do not have Endpoint Protection installed.

## How to run unscheduled antimalware scans

Endpoint Protection runs a quick scan of Dell Hybrid Cloud System for Microsoft resources every 24 hours, and runs a full scan once per week. You can start an unscheduled scan in the Endpoint Protection management tools in the Operations console as follows:

- 1 In the **Operations** console, in the **Monitoring** workspace, expand **Forefront Endpoint Protection**, and then click **Dashboard**.
- 2 In the **Tasks** pane, under **Protected Endpoint Tasks**, click either **Full Scan** or **Quick Scan**, depending on your preference, and how much time you want the scan to take.

**NOTE:** Be aware that a full scan on all Dell Hybrid Cloud System for Microsoft computers can affect performance. We recommend that you run unscheduled antivirus scans only outside of the system's peak usage hours.

## How to view scan results and respond to malware incidents

If Endpoint Protection finds malware on any target computers during scans, it raises alerts that you can view in the **Active Alerts** or **Dashboard** pages in Operations Manager. By default, Endpoint Protection automatically cleans malware. Alerts inform you that malware was found, and either disabled or removed. The following is an example of **Malware Cleaned** alert text.

### Malware Cleaned

**Alert Rule:** Malware Cleaned Alert Rule

**Alert Description:** Forefront Endpoint Protection detected and cleaned malware from 'ComputerName.DomainName.com'. No further action is needed.

### Malware Details:

**Threat Name:** Virus:DOS/EICAR\_Test\_File

**Threat Location:** containerfile:\_C:\SCEPTester\HarmlessInfectedFile;file:\_C:\SCEPTester\HarmlessInfectedFile->(UTF-16LE)

**More Information:** [http://go.microsoft.com/fwlink/?linkid=37020&name=Virus:DOS/EICAR\\_Test\\_File&threatid=2147519003](http://go.microsoft.com/fwlink/?linkid=37020&name=Virus:DOS/EICAR_Test_File&threatid=2147519003)

**Malware Severity:** Severe

## How to update antimalware definitions manually

By default, Endpoint Protection checks for updated antimalware definitions every eight hours. You should not need to update antimalware definitions manually; this is optional.

Antimalware updates are applied automatically by Windows Server Update Services (WSUS). Part of the initial installation and setup of Endpoint Protection included configuring WSUS to approve antivirus and antimalware updates automatically.

To update definitions manually, in the Operations console, do the following. We recommend that if you want to update antimalware definitions manually, you do this outside of peak usage hours:

- 1 In the **Monitoring** workspace, expand **Forefront Endpoint Protection**. Select either **Dashboard** or **Endpoints with FEP**.
- 2 Multi-select the computers on which you want to update antimalware definitions.
- 3 In the **Tasks** pane, under **Protected Endpoint Tasks**, click **Update Antimalware Definitions**.
- 4 In the **Update Antimalware Definitions** dialog box, verify the list of target computers, and then click **Run**.

## How to verify that updates are working

To verify that WSUS is applying current antivirus and antimalware definitions, review the logs in the Operations console:

- 1 In the **Monitoring** workspace, expand **Forefront Endpoint Protection**, and then click **Security Events**.
- 2 Look for Event ID (**Event Number**) 2000.

The following is a sample of a security event that shows the antimalware version number, with the current and previous signature version.

The screenshot shows a 'Details' window for a security event. The event is titled 'Current Signature Version: 1.203.686.0' and 'Previous Signature Version: 1.203.106.0', which are highlighted with an orange box. Other details include: Date and Time: 7/28/2015 10:06:02 AM; Log Name: System; Source: Microsoft Antimalware; Generating Rule: Collect Security Events Rule; Event Number: 2000; Level: Information; Logging Computer: computer.contoso.com; User: N/A; Description: %%860 signature version has been updated.; Signature Type: %%801; Update Type: %%804; User: NT AUTHORITY\NETWORK SERVICE; Current Engine Version: 1.1.11903.0; Previous Engine Version: 1.1.11903.0.

| Property                    | Value                                     |
|-----------------------------|-------------------------------------------|
| Date and Time:              | 7/28/2015 10:06:02 AM                     |
| Log Name:                   | System                                    |
| Source:                     | Microsoft Antimalware                     |
| Generating Rule:            | Collect Security Events Rule              |
| Event Number:               | 2000                                      |
| Level:                      | Information                               |
| Logging Computer:           | computer.contoso.com                      |
| User:                       | N/A                                       |
| Description:                | %%860 signature version has been updated. |
| Current Signature Version:  | 1.203.686.0                               |
| Previous Signature Version: | 1.203.106.0                               |
| Signature Type:             | %%801                                     |
| Update Type:                | %%804                                     |
| User:                       | NT AUTHORITY\NETWORK SERVICE              |
| Current Engine Version:     | 1.1.11903.0                               |
| Previous Engine Version:    | 1.1.11903.0                               |

Figure 71. Verify updates are working

## Managing certificates

It is recommended that you use a public key infrastructure (PKI) management tool to track the expiration and renewal of required certificates. By default, this is not installed as part of Dell Hybrid Cloud System for Microsoft.

The following are common management tasks for certificates. You will need to perform most of these tasks at regular intervals.



- View the certificates to determine whether or not certificates are self-signed, and when certificates will expire.
- If you have not already done so, replace self-signed certificates with CA-signed certificates to help improve the security of Dell Hybrid Cloud System for Microsoft.
- As certificates expire, you must periodically perform tasks in [Replacing self-signed certificates with CA-signed certificates](#) again.

## Viewing the certificates

You can view certificates in the GUI, by opening the `certlm.msc` snap-in on the Console VM, and targeting the snap-in at Dell Hybrid Cloud System for Microsoft computers that are running Windows Azure Pack website services, SMA, and SPF. These VMs are `<Prefix>APT01` and `<Prefix>APA01`.

## Replacing self-signed certificates with CA-signed certificates

The self-signed certificates that are generated as part of Dell Hybrid Cloud System for Microsoft installation are intended to be temporary. As a security best practice, if there are self-signed certificates still supporting Dell Hybrid Cloud System for Microsoft website services, you should promptly replace them with certificates that are issued by a trusted certification authority (CA), such as VeriSign or Thawte. The type of certificate you want for Dell Hybrid Cloud System for Microsoft website services is also called an SSL certificate.

You must also perform procedures in this section when you are updating expired certificates, as part of regular certificate management.

It is especially important that the following components use trusted certificates:

- Tenant portal
- Tenant public API
- Tenant authentication site
- Management portal for administrators
- SMA

Updating self-signed certificates to CA-signed certificates involves the following tasks:

- Step 1: Export the self-signed certificates to `.pfx` files, and create a folder tree for the certificates.
- Step 2: Obtain certificates from a trusted certification authority, and copy the `.cer` files to a share.
- Step 3: Import the trusted root and intermediate certification authority `.cer` files to establish the certificate chain on each VM.
- Step 4: Prepare the file share with the new `.pfx` certificates.
- Step 5: Update to the new trusted certification authority certificate on each component virtual machine.
- Step 6: Secure the shares that you created.

Each of these steps is described in the sections that follow.

## Step 1: Export self-signed certificates to .pfx files, and create a folder tree for the certificates

- 1 On the Console VM, create a Universal Naming Convention (UNC) file share to back up existing certificates:
  - a Create a folder, for example `C:\WAPCerts`.
  - b Right-click the folder, point to **Share with**, and then click **Specific people**.
  - c Type the user account `<Prefix>-System`, and then click **Add**.
  - d Under **Permission Level** for the `<Prefix>-System` account, click **Read**, and change it to **Read/Write**.
  - e Click **Share**, and then click **Done**.

The file share path is `\\<Prefix>CON01\WAPCerts`.

- 2 Sign in to the Windows Azure Pack management portal for administrators by using an account that is a member of the `<Prefix>-Ops-Admins` group.

- 3 Create a PowerShell Credential asset. The password for this asset is used to protect the private keys of the exported certificates.
  - a In the Windows Azure Pack management portal for administrators, click **Automation** in the navigation pane.
  - b On the **Automation** page, click **Assets**.
  - c Click **Add Setting**, and then click **Add Credential**.
  - d In the **Credential Type** list, click **PowerShell Credential**.
  - e In the **Name** box, type a name for the asset (for example, `CertExport`), and then click the **Next** arrow.
  - f In the **User Name** box, enter a user name; for example, `SMACred`. This does not need to be an existing user in the domain, or have any specific permissions.
  - g In the **Password** and **Confirm Password** boxes, type a password. This password is used to protect the private keys of the exported certificates.

 **IMPORTANT:** Record this password. If you must restore these certificates in the future, you need this password.

- 4 Run the **Get-SslCertificate** runbook:
  - a On the **Automation** page, click **Runbooks**.
  - b Search for the **Get-SslCertificate** runbook.
  - c With the **Get-SslCertificate** runbook selected, click **Start**.
  - d Specify the following parameters:

**Table 38. Get-SslCertificate runbook parameters**

| Input Parameter | Details                                                                                                                                                                                  |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ComputerNames   | Specify the computer names in JSON format, for example:<br><br><b>[ "&lt;Prefix&gt;APA01", "&lt;Prefix&gt;-APT01" ]</b><br><br>You must include the square brackets and quotation marks. |
| FileShare       | The UNC file share that you created in step 1 of this procedure; for example:<br><br><b>\\&lt;Prefix&gt;CON01\WAPCerts</b>                                                               |
| PFXCredential   | The name of the PowerShell Credential asset that you created in step 3; for example, <b>CertExport</b> .                                                                                 |

- 5 When the runbook finishes, browse the **WAPCerts** share to make sure there is output.  
The **Get-SslCertificate** runbook populates the file share with a folder tree in which the exported backups of the Personal Information Exchange File ( `.pfx` ) certificates are stored; for example:

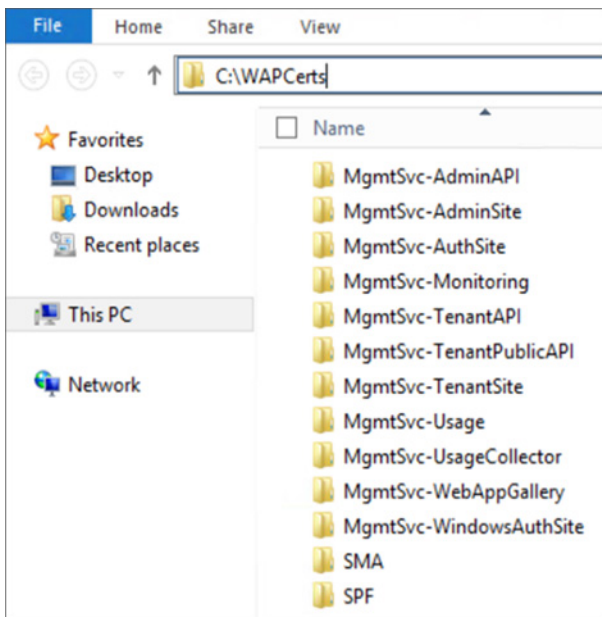


Figure 72. WAPCerts

The root folders for the Windows Azure Pack websites are named **MgmtSvc-\***, where **\*** is the name of the Windows Azure Pack service—for example, **MgmtSvc-TenantSite**.

In each root level folder, there is a second-level folder that is the name of the VM on which the certificate is installed. This folder contains the following files:

- The exported `.pfx` file
- A Java Script Object Notation (JSON) representation of the certificate—`.json` file
- A text file where you can view the certificate subject name, expiration date, and other information.

## Step 2: Obtain certificates from a trusted certification authority and copy the `.cer` files to a share

- 1 If you have not already, obtain one or more certificates from a trusted certification authority, as described in [Obtain a Certificate](#) on the Microsoft website.
- 2 On the Console VM, follow the same procedure that you did earlier to create a UNC file share for the trusted certification authority `.cer` files. For example, create a file share that is named `\\<Prefix>CON01\TCAShare`. Make sure that the `<Prefix>-System` account has Read/Write permissions.
- 3 Copy the certificate (`.cer`) file or files to the share location.

**NOTE:** Notice that there may be both a root certification authority certificate and an intermediate certification authority certificate.

## Step 3: Import the trusted root and intermediate certification authority `.cer` files to establish the certificate chain on each VM

This step establishes the correct certificate chain of trust on each VM. A certificate chain consists of all the certificates that are needed to certify the subject that is identified by the end certificate. For example, an intermediate certification authority certificate is linked to a root

certification authority certificate. To view the certificate chain, open the **Certificates** snap-in (**Certmgr.msc**), double-click the certificate, and then click the **Certification Path** tab.

- 1 In the Windows Azure Pack management portal for administrators, click **Automation**, and then click **Runbooks**.  
Depending on the number of certificates you have, and the certificate chain, you may have to run this runbook multiple times.

For example, say that you have one wildcard certificate that is registered at the domain level that you want to use for all sites on both VMs. It has an intermediate certification authority certificate and a root certification authority certificate. In this case, you would run the runbook two times.

- First, specify the share path of the root **.cer** file in **CerPathName**, and **Root** for **StoreName** in one run.
- Second, specify the share path of the intermediate **.cer** file for **CerPathName**, and **CA** as **StoreName** in the second run.

- 2 When you run the runbook, specify the following parameters:

**Table 39. Runbook parameters**

| Input Parameter | Details                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CerPathName     | The full path and file name where you saved the Internet Security Certificate ( <b>.cer</b> ) file in Step 2; for example, <code>\\&lt;Prefix&gt;CON01\TCAShare\filename.cer</code>                                                                                                                                                                                                |
| ComputerNames   | You must specify the computer names in JSON format. <ul style="list-style-type: none"> <li>• To import the <b>.cer</b> file to both VMs, specify:<br/><code>["&lt;Prefix&gt;APA01" , "&lt;Prefix&gt;-APT01"]</code></li> <li>• To import the <b>.cer</b> file to a single VM, specify:<br/><code>["&lt;Prefix&gt;APA01"]</code> or <code>["&lt;Prefix&gt;APT01"]</code></li> </ul> |
| StoreLocation   | For SSL certificates, type <code>LocalMachine</code> .                                                                                                                                                                                                                                                                                                                             |
| StoreName       | Possible values include: <ul style="list-style-type: none"> <li>• <b>Root</b><br/>Use this value for the Trusted Root Certification Authorities store.</li> <li>• <b>CA</b><br/>Use this value for the Intermediate Certification Authorities store</li> <li>• <b>MY</b><br/>Use this value for the Personal store.</li> </ul>                                                     |

## Step 4: Prepare the file share with the new .pfx certificates

### Prerequisites

- Before you do this step, make sure that the new certificates are in **.pfx** file format. If not, you can use the Certificates snap-in (**Certmgr.msc**) to convert them. For more information, see the TechNet article [Export a certificate with the private key \(http://technet.microsoft.com/library/cc737187\(v=ws.10\).aspx\)](http://technet.microsoft.com/library/cc737187(v=ws.10).aspx).
- Make sure that you know the password that was used to protect the private key.

### Procedure

- 1 On the Console VM, create a file share; for example, `\\<Prefix>CON01\ImportCerts`. Make sure that the `<Prefix>-System` account has Read/Write permissions.
- 2 Do either of the following:
  - If you are using one wildcard certificate for both VMs, and it is registered at the domain level (for example, `*.contoso.com`), go to Step 3.

- If you are using certificates that are registered at the website level, copy the folder tree from the share that you created in Step 1 to this new share, and then use the guidance in the next step to replace the existing **.pfx** files in the folder tree with the new ones. You could also create a similar folder tree in the new share, instead of copying the folder tree.
- 3 Prepare the **\\<Prefix>CON01\ImportCerts** file share with the new **.pfx** certificates. You can specify only one **.pfx** file per folder. Depending on the certificates that you have, do one of the following:
- If you have a wildcard certificate for the domain (for example, \*.contoso.com), you only need to copy the **.pfx** file to the share, for example: **\\<Prefix>CON01\ImportCerts\contoso.com.pfx**. This layout is the quickest way to update all websites with the same SSL certificate.
  - You can also add the **.pfx** files at the VM level. For example:

```

\\<Prefix>CON01\ImportCerts

\MgmtSvc-AdminAPI
<Prefix>APA01
 CF75D3CAE126353B0700F9820ECBA0F67F75001C.pfx

\MgmtSvc-AdminSite
<Prefix>APA01
 CF75D3CAE126353B0700F9820ECBA0F67F75001C.pfx

\MgmtSvc-AuthSite
<Prefix>APT01
 CF75D3CAE126353B0700F9820ECBA0F67F75001C.pfx

\MgmtSvc-Monitoring
<Prefix>APA01
 CF75D3CAE126353B0700F9820ECBA0F67F75001C.pfx

\MgmtSvc-TenantAPI
<Prefix>APA01
 CF75D3CAE126353B0700F9820ECBA0F67F75001C.pfx

\MgmtSvc-TenantPublicAPI
<Prefix>APT01
 CF75D3CAE126353B0700F9820ECBA0F67F75001C.pfx

\MgmtSvc-TenantSite
<Prefix>APT01
 CF75D3CAE126353B0700F9820ECBA0F67F75001C.pfx

\MgmtSvc-Usage
<Prefix>APA01
 CF75D3CAE126353B0700F9820ECBA0F67F75001C.pfx

\MgmtSvc-UsageCollector
<Prefix>APA01
 CF75D3CAE126353B0700F9820ECBA0F67F75001C.pfx

\MgmtSvc-WebAppGallery
<Prefix>APA01
 CF75D3CAE126353B0700F9820ECBA0F67F75001C.pfx

\MgmtSvc-WindowsAuthSite
<Prefix>APA01
 CF75D3CAE126353B0700F9820ECBA0F67F75001C.pfx

\SMA
<Prefix>APA01
 CF75D3CAE126353B0700F9820ECBA0F67F75001C.pfx

\SPF
<Prefix>APA01
 CF75D3CAE126353B0700F9820ECBA0F67F75001C.pfx

```

The **Set-SslCertificate** runbook that you run in the next section processes the folder tree in the following order:

- Searches for `.pfx` files at `\\host\share\WebSiteName\VMName\*.pfx`
- If it finds no `.pfx` files at the VM level, it searches `\\host\share\WebSiteName\*.pfx`
- If it finds no `.pfx` files at the website level, it searches `\\host\share\*.pfx`
- If it finds no `.pfx` files at all, it returns the following error message: **Error, no .pfx file**

## Step 5: Update to the new trusted certification authority certificate on each component virtual machine

You must run a runbook to update to the new, signed certificates for the Windows Azure Pack website services, SMA, and SPF.

- 1 Create a PowerShell Credential asset. The password for this asset must match the password that was used to protect the private key of the new certificates.

**NOTE:** If you want to restore a certificate, this password must match the password you used in [Step 1](#).

- a In the Windows Azure Pack management portal for administrators, click **Automation** in the navigation pane.
  - b On the **Automation** page, click **Assets**.
  - c Click **Add Setting**, and then in the **Add Setting** window, click **Add Credential**.
  - d In the **Credential Type** list, click **PowerShell Credential**.
  - e In the **Name** box, type a name for the asset (for example, `CertImport`), and then click the **Next** arrow.
  - f In the **User Name** box, enter a user name; for example, `SMACred`. This does not need to be an existing user in the domain, or have any specific permissions.
  - g In the **Password** and **Confirm Password** boxes, type a password. This password must match the password that was used to protect the private key of the certificates that you want to import.
- 2 Run the **Set-SslCertificate** runbook to update to the new trusted certification authority certificate. The SSL certificates must be provided as `.pfx` files, and must include a private key protected by a password. The runbook takes the following parameters:

**Table 40. Set-SslCertificate runbook parameters**

| Input Parameter | Details                                                                                                                                                                                                                                                                                                                                             |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ComputerNames   | You must specify the computer names in JSON format. <ul style="list-style-type: none"> <li>• To update the certificates on both VMs, specify: <pre>["&lt;Prefix&gt;APA01" , "&lt;Prefix&gt;-APT01"]</pre> </li> <li>• To update the certificates on a single VM, specify: <pre>["&lt;Prefix&gt;APA01"] or ["&lt;Prefix&gt;APT01"]</pre> </li> </ul> |
| Fileshare       | The UNC file share that you created in the previous procedure to store the new <code>.pfx</code> certificates; for example, <code>\\&lt;Prefix&gt;CON01\ImportCerts</code>                                                                                                                                                                          |
| PFXCredential   | The name of the PowerShell Credential asset that you created in the first step of this procedure; for example, <code>CertImport</code>                                                                                                                                                                                                              |

**NOTE:** Each time that you run the runbook, even if the runbook has a status of **Completed**, make sure that you check the output for errors.

## Step 6: Secure the shares that you created

You should take steps to secure the shares where you stored the certificate information. Or, alternately, you can remove sharing completely, if so desired.

You can now:

- Archive these files to a different location, or
- Delete the files after confirming that all new certificates are working, that is, administrators and tenants are able to sign in and work in their Windows Azure Pack management portals.

The shares where you stored certificate information were:

- \\<Prefix>CON01\WapCerts
- \\<Prefix>CON01\TCAShare
- \\<Prefix>CON01\ImportCerts

## Updating certificates about to expire

To update certificates that are about to expire, follow the procedures described in [Replacing self-signed certificates with CA-signed certificates](#).

# Appendix A: Expanding the stamp

When customers initially purchase the Dell Hybrid Cloud System for Microsoft, the solution may be configured with fewer than the maximum number of compute nodes, storage JBODs, network switches, or backup hosts. The following figure outlines the components that may be ordered to expand the scale and/or functionality of the solution after it has already been deployed. This section outlines procedures for adding these components and integrating them into the solution.

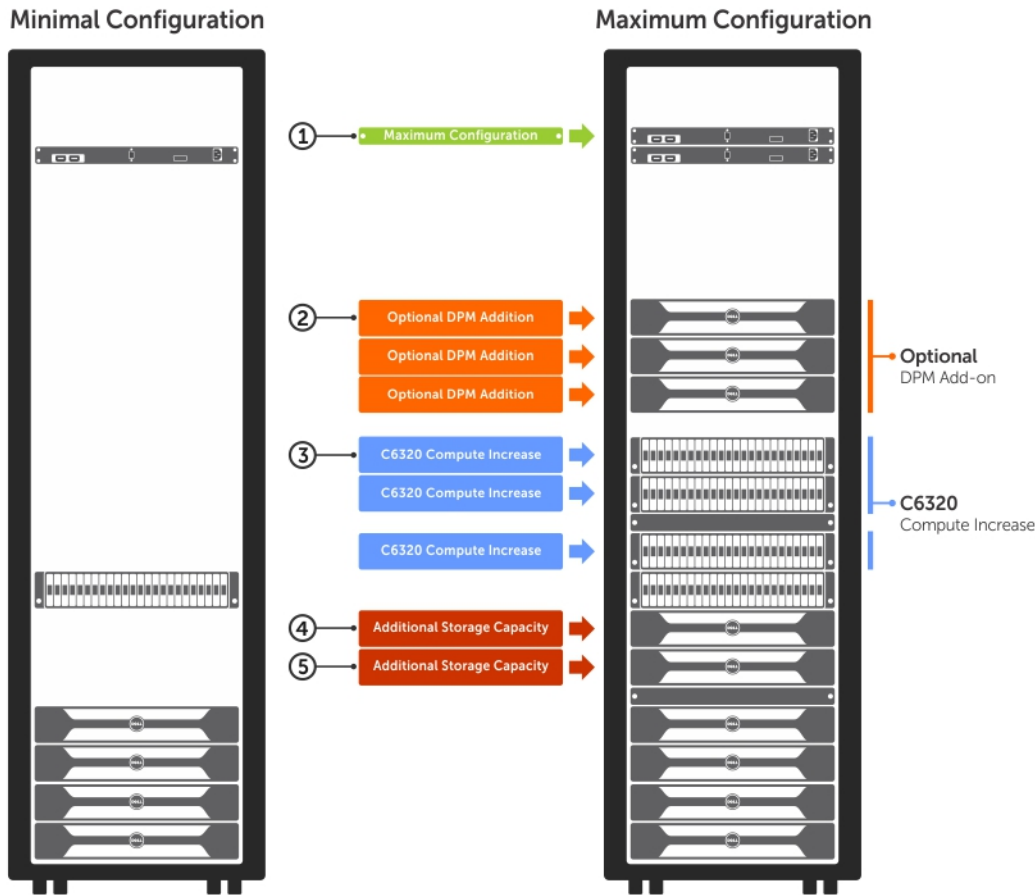


Figure 73. Expansion of Dell Hybrid Cloud System for Microsoft

Topics:

- [Compute expansion workflow](#)
- [Adding another server to backup infrastructure](#)

## Compute expansion workflow

The number of compute nodes in the solution can scale from a single chassis (with four PowerEdge C6320 servers) up to four chassis (for a total of 16 servers). The unit of scalability is a complete chassis, so nodes must be added four at a time. The chassis must go through the Dell Integration Center and be preconfigured and imaged in the same manner as the original nodes.



However, if a significant amount of time has passed between the original order and the expansion, it is likely that image versions and/or firmware versions may be different. Before beginning the expansion deployment, it will then be necessary to bring the existing environment up to a solution release level that is compatible with the images provided on the expansion chassis. The Patch and Update (P&U) process can be used to update the solution stack.

For more information about P&U, go to the Dell support website at [support.dell.com](http://support.dell.com). Click **Choose from all Products > Servers, Storage, & Networking > Engineering Solutions > Microsoft Cloud Solutions > Dell Hybrid Cloud System for Microsoft**. P&U packages and documentation are released to that site when available.

**NOTE:** Because they require imaging before they are delivered, compute nodes and backup nodes are shipped from the Dell Integration Centers. All other components ship directly to the customer without any customization.

## Physical installation

Install the compute chassis into the rack unit above the upper-most chassis that is currently deployed in the solution. Run the power cables from the chassis to the PDU, and connect the 10GbE ports on each C6320 server to the appropriate ports on the Dell Networking S4048-ON switches.

## Deploying compute expansion nodes

The Deployment user interface remains installed on the console VM (<prefix>CON01) and is used to start the **DeployDriver** for compute expansion. Consult with your Dell technical support representative to find out how to deploy compute expansion nodes for your implementation of the Dell Hybrid Cloud System for Microsoft.

**NOTE:** Compute expansion is implemented by Dell Services.

## Adding another server to backup infrastructure

You can add DPM backup servers to an existing Dell Hybrid Cloud System for Microsoft backup infrastructure. Deployment of the backup servers is implemented by Dell Services. You can expand up to three backup servers.

After you run the **BackupDeployDriver** script, run the **Complete-BackupDeployment** runbook. You do not have to run the **Protect-ManagementComponents** runbook.

Then, you may have to run P&U to ensure that the latest updates are applied, and that the stamp and backup infrastructure are at the same version.

Use the following guidance to determine if and when a P&U run is required:

**Table 41. Conditions for P&U run**

| Conditions                                          | P&U run required?                                                                                                                                                                                                               |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Stamp is at same version as the new backup host.    | A P&U run is not required after you add the backup host.                                                                                                                                                                        |
| Stamp has a later version than the new backup host. | Run a required P&U <b>after</b> you add the backup host.                                                                                                                                                                        |
|                                                     | <b>NOTE:</b> Starting with Update 1611, you can target P&U to run against only the new backup hosts. For more information, see <i>DHCS Patch and Update Framework for 1703</i> at the location where you find approved updates. |
| New backup host has a later version than the stamp. | <b>Before</b> you add the backup host, run a required P&U to update the stamp to the same version as the new host.                                                                                                              |

To check the Microsoft update version on a new node, open the file `C:\Program Files\Microsoft Cloud Solutions\Version.xml` on the host.

To check the Microsoft update version on the stamp, see [How to check which update package is installed](#).

# Appendix B: Performing a factory reset

This section describes how to reset a deployed Dell Hybrid Cloud System for Microsoft stamp so that it can be redeployed.

Before you redeploy, you must reset backup servers, storage servers, and compute nodes to factory defaults and prepare for a fresh deployment.

**△ CAUTION: Performing these steps results in loss of all workload VMs running in your private cloud. Before you reset the stamp, please make sure all important tenant VMs have been moved to another private, hosted, or public cloud. Do not move management VMs. They are redeployed from initial state.**

Topics:

- [Access and account requirements](#)
- [Resetting the backup servers](#)
- [Resetting the storage cluster \(<Prefix>-SCL\)](#)
- [Resetting the compute cluster \(<Prefix>CCL\)](#)
- [Clean up Active Directory and DNS records](#)
- [Clean up artifacts created by Azure Site Recovery](#)

## Access and account requirements

### Prerequisites

- To perform the steps described in the following sections, you need console access to each physical server in your cloud. You can access a console either:
  - Directly, by using a keyboard and a monitor attached to each server, or
  - Over a remote console connection made through the Integrated Dell Remote Access Controller (iDRAC).
- Factory reset procedures depend on the type of server you want to reset. There are different procedures for:
  - Backup hosts
  - Storage hosts
  - Compute hosts.
- To perform cleanup steps, you need a domain user account with:
  - Permissions to remove the Active Directory organizational unit (OU) for Dell Hybrid Cloud System for Microsoft (including all child objects), and
  - Permissions to remove records in DNS.

**△ CAUTION: Do not clean up your Active Directory (AD) and Domain Naming System (DNS) until after you have completed the steps outlined in the following sections. For information on cleanup steps, see [Clean up Active Directory and DNS records](#).**

Perform the following steps on each physical computer in your private cloud:

- Backup Servers
- Storage Servers
- Compute Servers.

# Resetting the backup servers

**CAUTION:** Before you start the factory reset for Backup Servers, make sure that you are using a Microsoft System Center Server product key, the Volume License Key. See the *Solution Integration Document (SID) for Volume License Key* information. If you are not using the Volume License Key, Backup Server deployment will fail after a reset as well.

- 1 Open iDRAC consoles for each physical host. The Field Engineer (FE) must be connected using the FE laptop. It is connected to Port TE 1/40 on one of the Top of Rack switches. Configure the laptop with the IP in the *Solution Integration Document*.
- 2 Log in to the backup host **<Prefix>B01** with an account that has Local Administrator permissions, for example, as a member of the **<Prefix>-Ops-Admins** group.
- 3 For the backup server, make sure that you **Clear the Partition** for the Raid 6, that is, the partition that is created to save backed up data.
- 4 Start the PowerShell by using the `Start PowerShell` command.

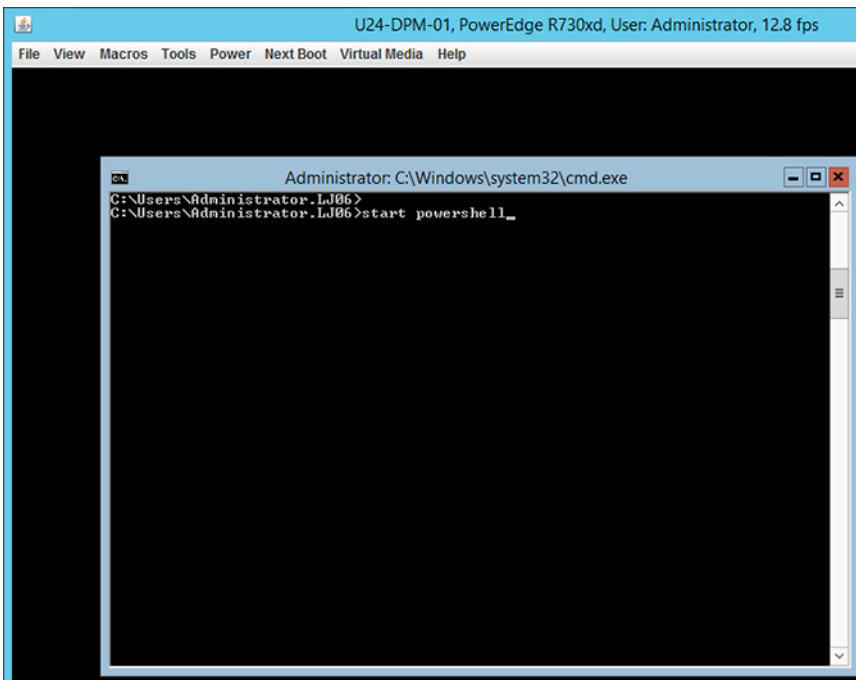


Figure 74. Start PowerShell

- 5 Once the PowerShell is started, get a list of disks by entering the **Get-disk** command.

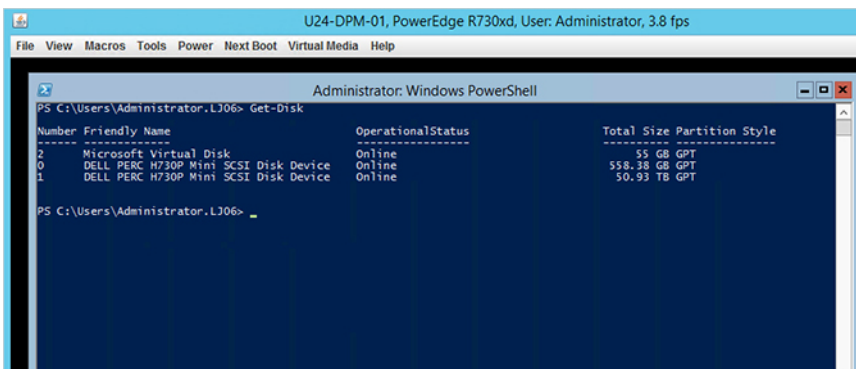


Figure 75. Get-disk

The command returns a list of disks with their status and size.

- As indicated in the graphic, **Disk #1** requires clearing. To confirm that this disk is the backup disk, obtain a list of partitions by entering the command **Get-Partition**.

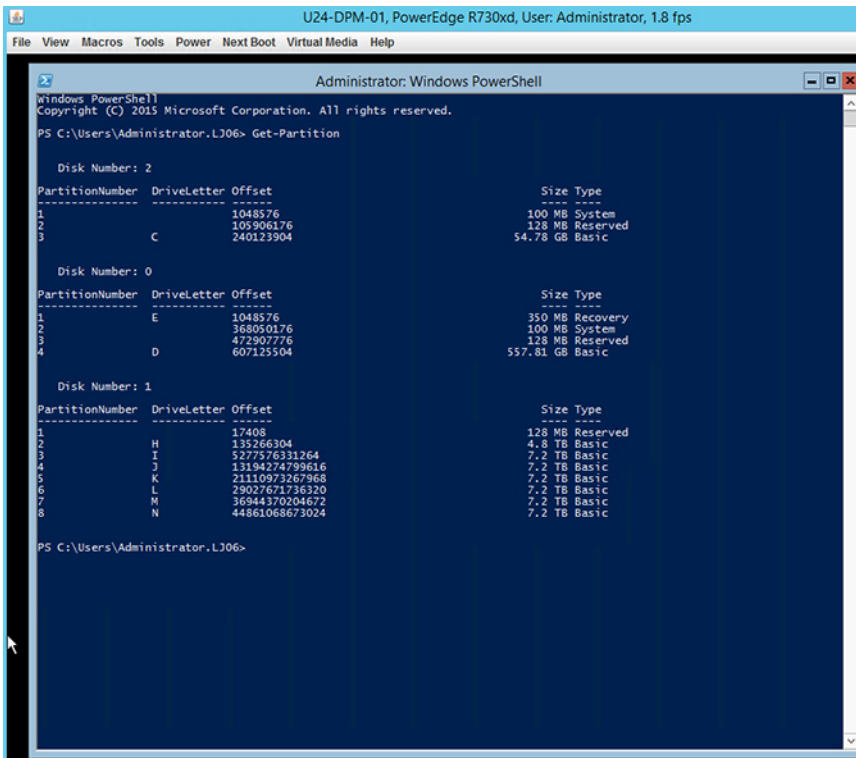


Figure 76. Get-partition

The list of partitions that is returned confirms that **Disk #1** has the partition created to house the backed-up data.

- Now delete **Disk #1** and clean out all its data by entering the following PowerShell cmdlet:  
`Clear-Disk -Number 1 -RemoveData -Verbose`
- Select **Yes** to proceed.

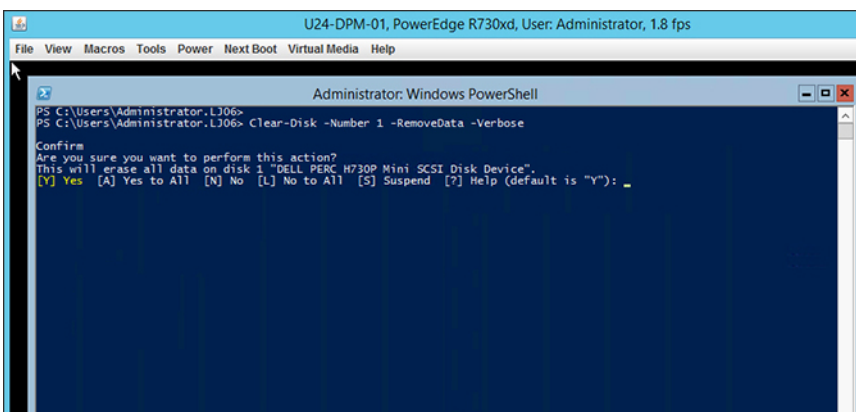
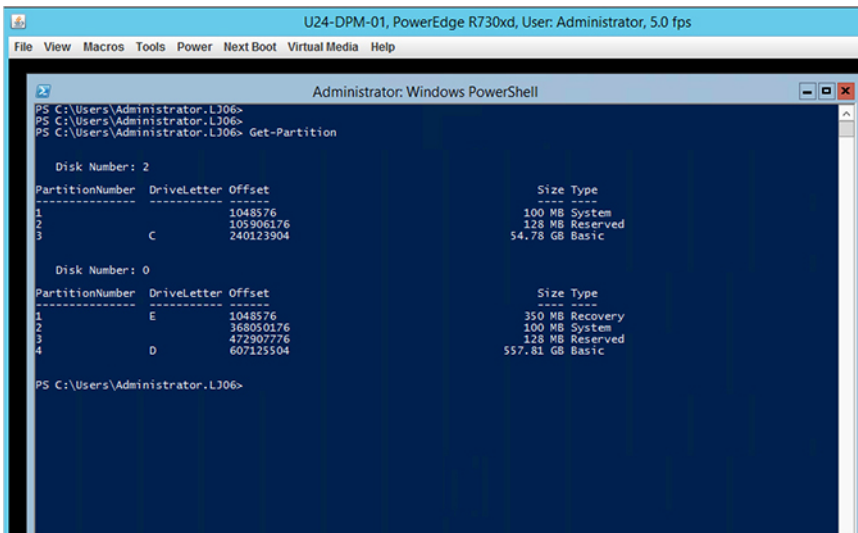


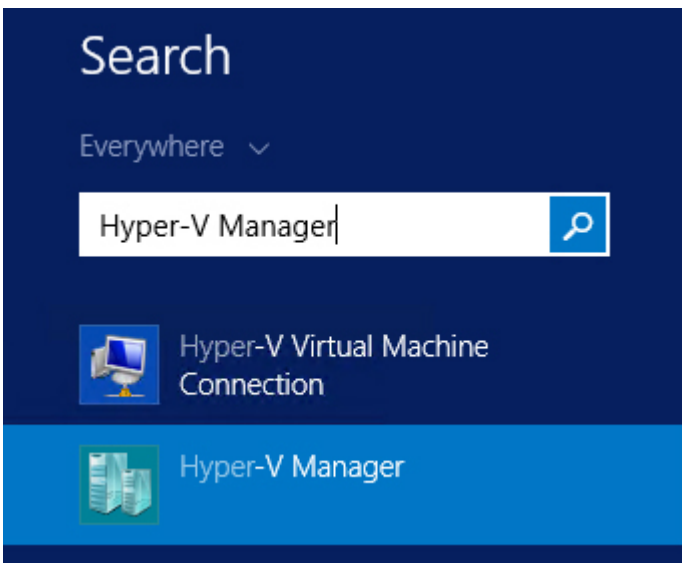
Figure 77. Proceed to clear disk

- After the disk has been cleared, run the **Get-Partition** PowerShell cmdlet again to confirm that the partitions and **Disk #1** have been cleared and removed.



**Figure 78. Confirmation disk is removed**

- 10 Log on to the Console VM **<Prefix>CON01** with Domain Account. For Domain Account information, see the ***Solution Integration Document***
- 11 Remove the host from VMM.
  - a In the VMM console, open the **VMs and Services** workspace.
  - b Under the **All Hosts** host group, remove the backup host on which the DPM VM resides.
- 12 Remove the backup host and DPM VMs from Operations Manager.
  - a Open the Operations Console.
  - b In the **Administration** workspace, expand **Device Management > Agent Managed**.
  - c Right-click the corrupted DPM server, and then click **Delete**.
- 13 Click **Start** and search for **Hyper-V Manager** Now you must connect to the Backup Host **<Prefix>B01** and delete the running virtual machine for **<Prefix>DPM01** and **<Prefix>DPM02**.



**Figure 79. Search and connect to server using Hyper-V Manager**

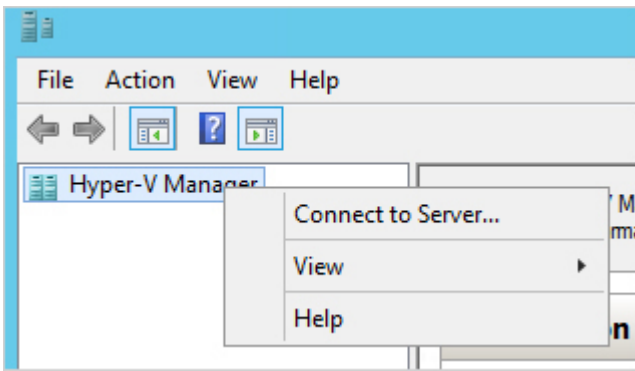


Figure 80. Connect to Server

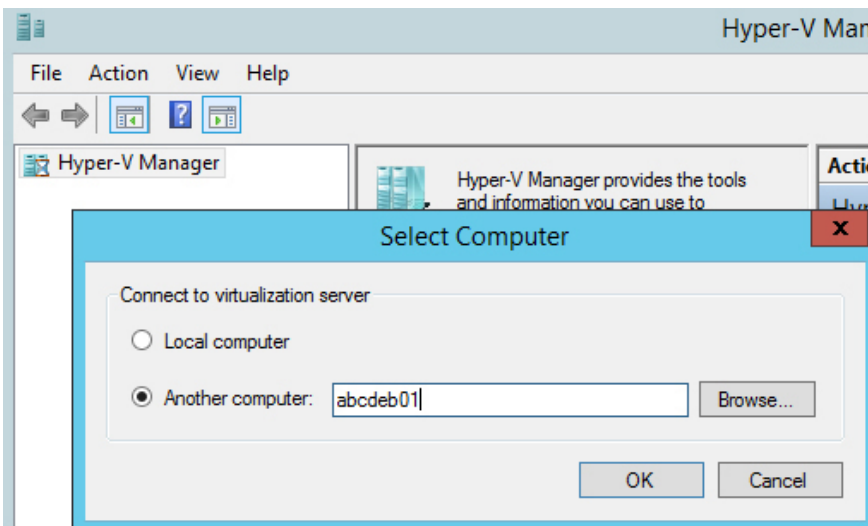


Figure 81. Select Server

- 14 Next remove the **<Prefix>DPM01** and **<Prefix>DPM02** virtual machine folders from the Backup Host **<Prefix>B01**. To accomplish this, access your Backup Host **<Prefix>B01** from the **Console VM** as follows:
  - a Click **Start** and search for **Run**.
  - b Access the **D:** drive of the Backup Host **<Prefix>B01** by typing `\\<Prefix>B01\d$`.
  - c Delete the folders **<Prefix>DPM01** and **<Prefix>DPM02**.

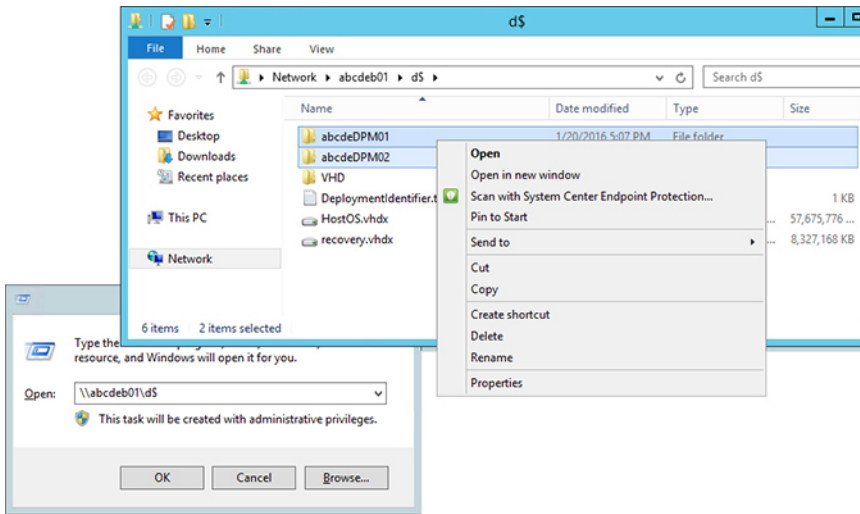


Figure 82. Delete folders from backup host

- 15 At the PowerShell prompt, run the `reagentc /bootlore` command.  
If you receive a message saying **REAGENTC.EXE: Operations successful**, continue to the next step. If you do not receive this message, follow the escalation path.

**NOTE:** If this is not the first time the server has been reset, you might receive an error message saying: **REAGENTC.EXE: Windows RE is disabled.** In that case, open an elevated Windows PowerShell session, and run the `reagentc /enable` command. If you receive a message saying **REAGENTC.EXE: Operations successful**, enter `reagentc /bootlore`. If you do not receive the “Operations successful” message, follow the escalation path.

- 16 In a command window, enter `Shutdown -r -t 0`.  
The server restarts.
- 17 When the server restarts in the **Windows Recovery Environment**, click **Troubleshoot**.

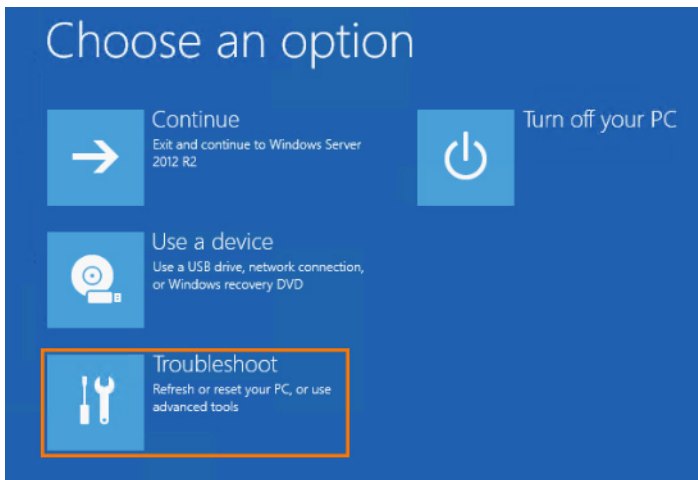


Figure 83. Windows Recovery Environment menu

- 18 On the **Troubleshoot** menu, click **Advanced options**.



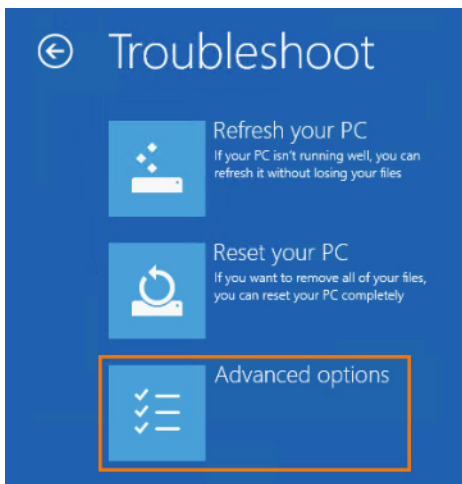


Figure 84. Troubleshoot advanced

- 19 In **Advanced options**, click **Command Prompt**.

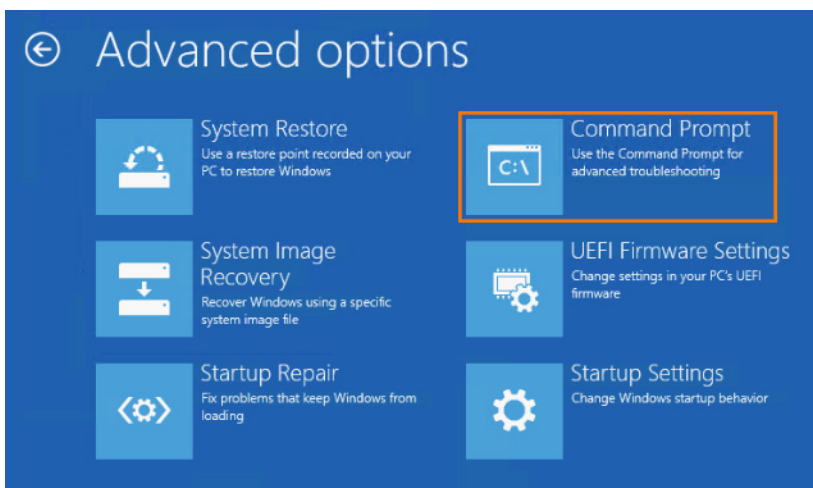


Figure 85. Advanced options

- 20 When a system command prompt is displayed, run the following commands:

```
del c:\hostos.vhdx
```

```
copy c:\recovery.vhdx c:\hostos.vhdx
```

- 21 Close the command prompt by typing **Exit**.
- 22 On the **Windows Recovery Environment** main menu, click **Continue**.

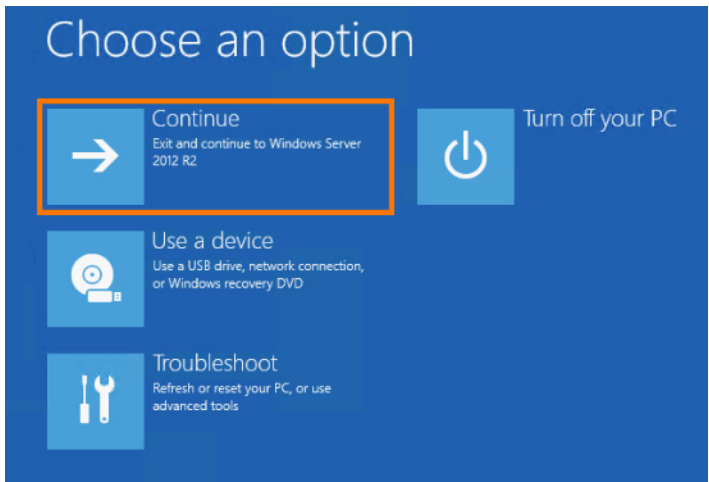


Figure 86. Troubleshoot options

The server restarts and completes factory first-boot automation.

**CAUTION:** After completing this factory reset process, wait for at least 30 minutes before proceeding to the next step.

- 23 From the iDRAC Virtual Console, select **Power > Graceful Shutdown**.

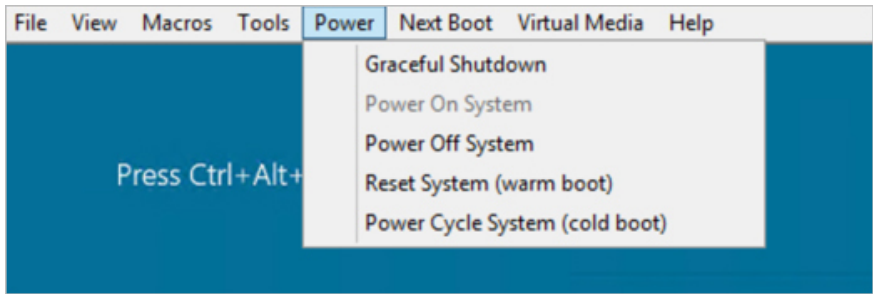


Figure 87. iDRAC graceful shutdown

The backup hosts power off. Later in the factory reset process, you follow the power-on procedures for Dell Hybrid Cloud System for Microsoft, as described in [Starting up the stamp](#).

## Resetting the standalone backup host

Before starting this procedure, you must follow the steps in [Resetting the backup servers](#).

- NOTE:** If you need to perform a factory reset for just the Backup Host, perform the following steps after you have performed the steps in [Resetting the backup servers](#).

After a failed backup deployment, you must perform the following steps to clean the environment for a fresh backup deployment.

- 1 Clean the Active Directory objects for **<Prefix>B01**, **<Prefix>DPM01**, and **<Prefix>DPM02**.
  - a Log in to the customer's Domain Control and delete the entries for **<Prefix>B01**, **<Prefix>DPM01**, **<Prefix>DPM02**. In the following example, the Dell Hybrid Cloud System environment is called "abcde."

| Name         | Type     |
|--------------|----------|
| abcdeAPA01   | Computer |
| abcdeAPT01   | Computer |
| ABCDEB01     | Computer |
| ABCDEC21A    | Computer |
| ABCDEC21B    | Computer |
| ABCDEC21C    | Computer |
| ABCDEC21D    | Computer |
| abcdeCCL     | Computer |
| ABCDECON01   | Computer |
| abcdeDPM01   | Computer |
| abcdeDPM02   | Computer |
| abcdeOM01    | Computer |
| ABCDE55      | Computer |
| ABCDE57      | Computer |
| abcdeSCL     | Computer |
| abcdeSFS     | Computer |
| abcdeSQL01   | Computer |
| abcdeSQL02   | Computer |
| abcdeSQLCL   | Computer |
| abcdeSQLIN01 | Computer |

Figure 88. Backup Active Directory cleanup

- 2 Clean the DNS objects for <Prefix>B01, <Prefix>DPM01, and <Prefix>DPM02.
  - a Log in to the customer’s DNS server, and delete the entries for <Prefix>B01, <Prefix>DPM01, and <Prefix>DPM02. In the following example, Dell Hybrid Cloud System environment is called “abcde.”

| Name                    | Type                     | Data                           | Timestamp            |
|-------------------------|--------------------------|--------------------------------|----------------------|
| (same as parent folder) | Start of Authority (SOA) | [1614], j06-dc1.j06.lab., h... | static               |
| (same as parent folder) | Name Server (NS)         | j06-dc1.j06.lab.               | static               |
| (same as parent folder) | Host (A)                 | 192.168.26.122                 | 1/22/2016 7:00:00 AM |
| _msdcs                  |                          |                                |                      |
| _sites                  |                          |                                |                      |
| _tcp                    |                          |                                |                      |
| _udp                    |                          |                                |                      |
| abcdeAPA01              | Host (A)                 | 192.168.26.29                  | 1/26/2016 2:00:00 PM |
| abcdeAPT01              | Host (A)                 | 192.168.26.30                  | 1/26/2016 2:00:00 PM |
| abcdeB01                | Host (A)                 | 192.168.26.35                  | 1/20/2016 5:00:00 PM |
| abcdeC21A               | Host (A)                 | 192.168.26.25                  | 1/26/2016 1:00:00 PM |
| abcdeC21B               | Host (A)                 | 192.168.26.26                  | 1/26/2016 1:00:00 PM |
| abcdeC21C               | Host (A)                 | 192.168.26.27                  | 1/26/2016 1:00:00 PM |
| abcdeC21D               | Host (A)                 | 192.168.26.28                  | 1/26/2016 1:00:00 PM |
| abcdeCCL                | Host (A)                 | 192.168.26.31                  | 1/26/2016 1:00:00 PM |
| abcdeCON01              | Host (A)                 | 192.168.26.20                  | 1/27/2016 6:00:00 AM |
| abcdeDPM01              | Host (A)                 | 192.168.26.36                  | 1/20/2016 5:00:00 PM |
| abcdeDPM02              | Host (A)                 | 192.168.26.37                  | 1/20/2016 5:00:00 PM |

Figure 89. Backup DNS cleanup

- 3 Delete Backup Deployment registry entries for <Prefix>B01, <Prefix>DPM01, and <Prefix>DPM02.
  - a Log in to the <Prefix>CON01 console VM with the Domain account. For Domain account information, see the *Solution Integration Document* (SID).
  - b Once you are logged in, open the registry editor. To do this, click the Windows **Start** button and search for **regedit**.
  - c Browse to the HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Cloud Solutions\Deployment\Status registry key, and delete the entries for <Prefix>B01, <Prefix>DPM01, and <Prefix>DPM02.

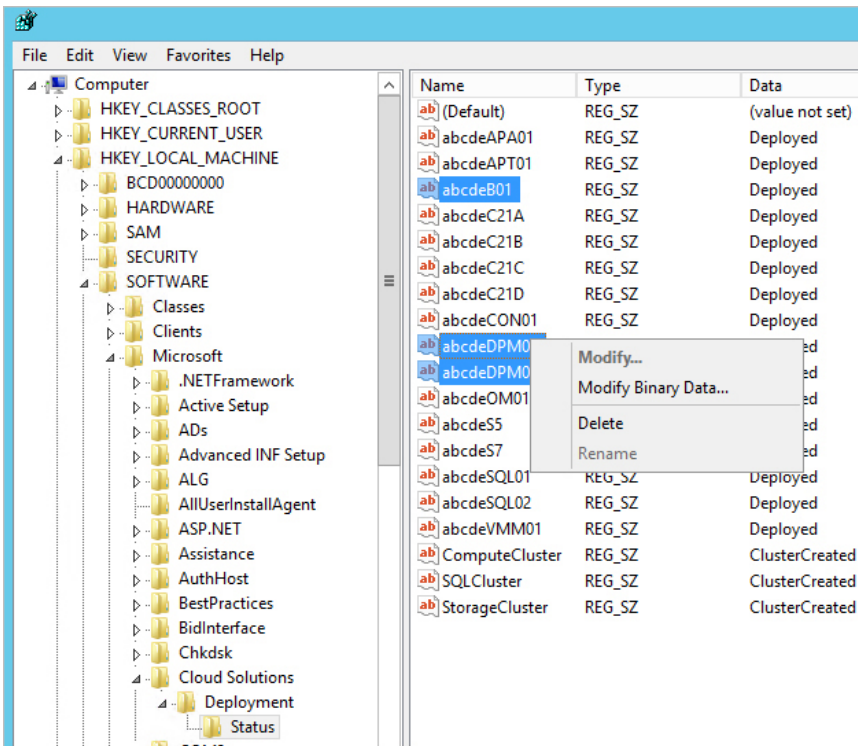


Figure 90. Backup registry cleanup

- 4 Delete all backup-related configuration for **<Prefix>B01**, **<Prefix>DPM01**, and **<Prefix>DPM02** in deploymentmanifest.xml.
  - a Open the manifest file on the **<Prefix>CON01** console VM located at C:\Program Files\Microsoft Cloud Solutions\DeployDriver\Manifests\ deploymentmanifest.xml. Search (CTRL+F ) for the following sections and delete them.
 

**<BackupConfiguration>.....<BackupConfiguration>** and **<BackupVMs>.....<BackupVMs>**

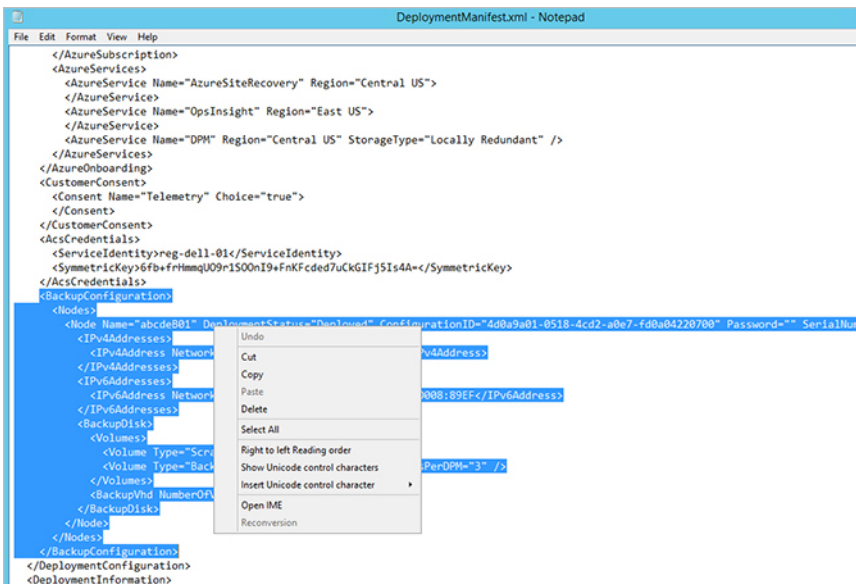
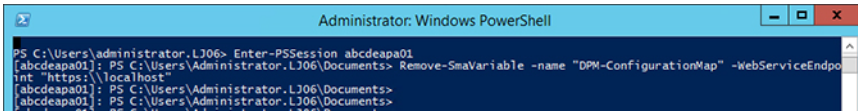


Figure 91. Backup manifest cleanup

- 5 On the **<Prefix>APA01** server, run the **Remove SMA variable** command in a PowerShell.

While you are logged in to the **<Prefix>CON01** console VM using the Domain Credentials (see the *Solution Integration Document*), remotely connect to the **<Prefix>APA01** server using the PowerShell command **Enter-Psession <Prefix>APA01**. When connected, use the command **Remove-SmaVariable -name "DPM-ConfigurationMap" -WebServiceEndpoint "https://localhost"**.



```
Administrator: Windows PowerShell
PS C:\Users\administrator.LJ06> Enter-PSSession abcdeapa01
[abcdeapa01]: PS C:\Users\Administrator.LJ06\Documents> Remove-SmaVariable -name "DPM-ConfigurationMap" -WebServiceEndpoint "https://localhost"
[abcdeapa01]: PS C:\Users\Administrator.LJ06\Documents>
[abcdeapa01]: PS C:\Users\Administrator.LJ06\Documents>
```

Figure 92. PowerShell Remove-SmaVariable

The SMA variable is removed from the **<Prefix>APA01** server.

- 6 Re-run **BackupDeployDriver**.

## Resetting the storage cluster (**<Prefix>-SCL**)

- 1 Open iDRAC consoles for each physical host.

The Field Engineer (FE) must be connected using the FE laptop. The laptop is connected to port TE 1/40 on one of the Top of Rack switches.

- 2 Configure the FE laptop with the IP address in the *Solution Integration Document* (SID).

- 3 Power down the JBODs.

These are the MD1420 or MD1400 storage enclosures.

- 4 Launch the iDRAC Virtual Console for the first Storage Host.

- 5 Log on to the server with an account that has Local Administrator permissions, for example, as a member of the **<Prefix>-Diag-Admins** group.

- 6 Open an elevated command prompt, and run the **reagentc /bootore** command.

If you receive a message saying **REAGENTC.EXE: Operations successful**, continue to the next step. If you do not receive this message, follow the escalation path.

**NOTE:** If this is not the first time the server has been reset, you might receive the error message: **REAGENTC.EXE: Windows RE is disabled. In that case, open an elevated Windows PowerShell session, and run the following commands:**

- **Stop-Service clussvc**
- **reagentc /enable**
- If you receive the message: **REAGENTC.EXE: Operations successful**, enter **reagentc /bootore**. If you do not receive the **Operations successful** message, follow the escalation path.

- 7 In the open Command prompt window, type **Shutdown -r -t 0**.

The server restarts.

- 8 When the server restarts in the **Windows Recovery Environment** click **Troubleshoot**.

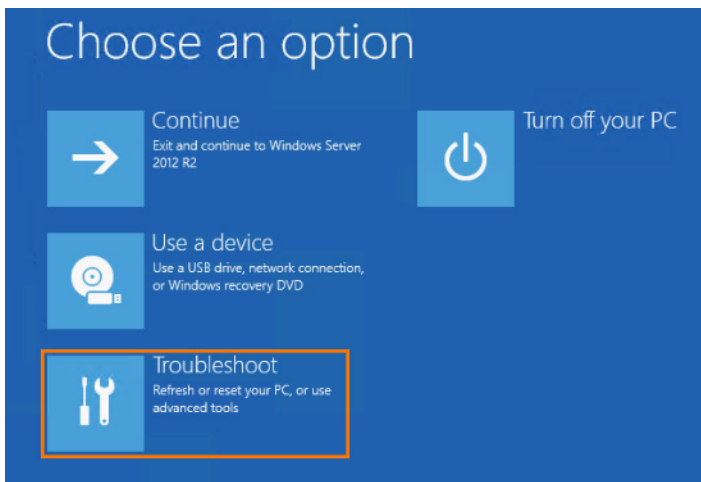


Figure 93. Troubleshoot options

- 9 On the **Troubleshoot** menu, click **Advanced options**.

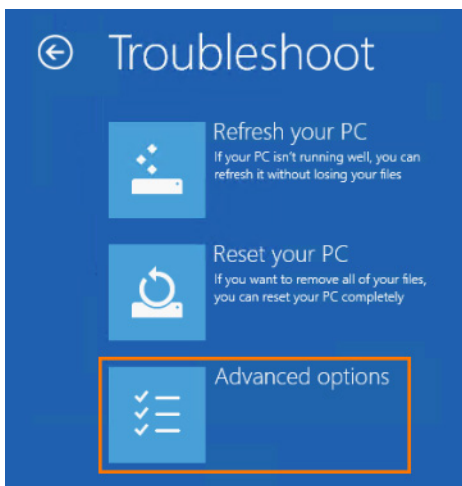
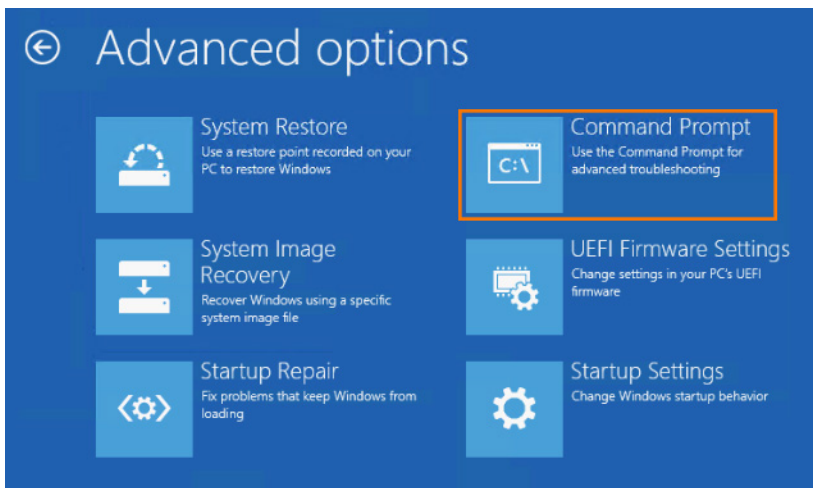


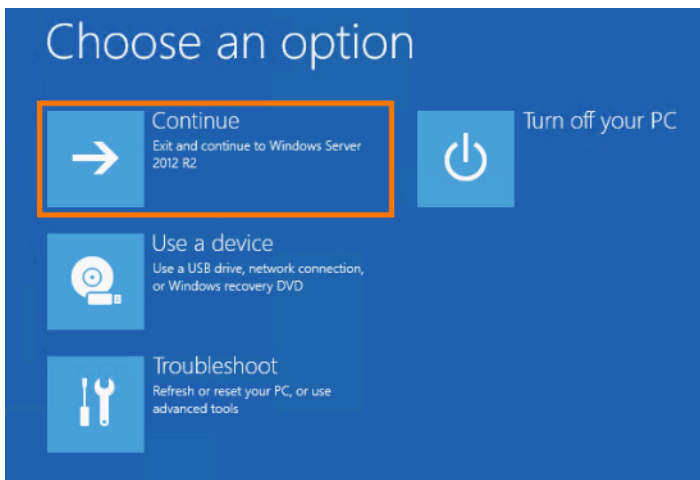
Figure 94. Troubleshoot advanced

- 10 In **Advanced options**, click **Command Prompt**.



**Figure 95. Advanced options**

- 11 When a system command prompt displays, change to the C: drive and run the following commands:
  - `del c:\hostos.vhdx`
  - `copy c:\recovery.vhdx c:\hostos.vhdx`
- 12 Close the command prompt by typing **Exit**.
- 13 On the **Windows Recovery Environment** main menu, click **Continue**.



**Figure 96. Troubleshoot options**

The server restarts and completes factory first-boot automation.

**⚠ CAUTION:** After completing this factory reset process, wait for at least 30 minutes before proceeding to the next step.

- 14 From the **iDRAC Virtual Console**, select **Power > Graceful Shutdown**.



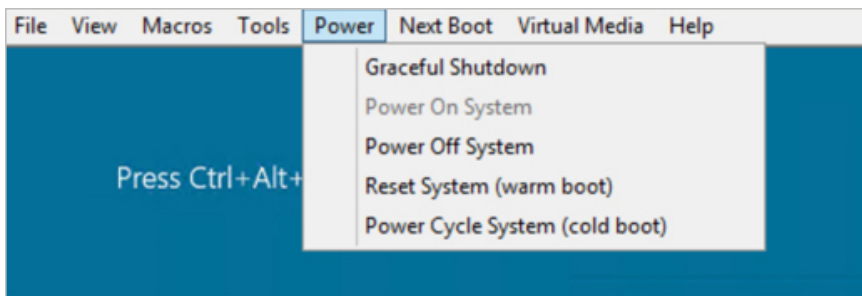


Figure 97. iDRAC Graceful Shutdown

The storage hosts power off. Later in the factory reset process, you follow the power-on procedures for Dell Hybrid Cloud System for Microsoft, as described in [Starting up the stamp](#).

**NOTE:** Upon completion of the factory reset process, manually power off the (MD14xx) JBODs that are connected to the R730s.

## Resetting the compute cluster (<Prefix>CCL)

- 1 Open iDRAC Consoles for each physical host. Connect the Field Engineer (FE) laptop. It is connected to Port TE 1/40 on one of the Top of Rack switches. Configure the laptop with the IP in the *Solution Integration Document* (SID).
- 2 Log on to the server with an account that has local Administrator permissions, for example, as a member of the <Prefix>-Diags-Admins group.
- 3 Open an elevated command prompt, and run the following command:

```
reagentc /boottore
```

- 4 If you receive a message saying **REAGENTC.EXE: Operations successful**, continue to the next step.

**NOTE:** If this is not the first time the server has been reset, you might receive an error message saying: **REAGENTC.EXE: Windows RE is disabled**. In that case, open an elevated Windows PowerShell session, and run the following commands:

- Stop-Service clussvc
- reagentc /enable
- If you receive a message saying **REAGENTC.EXE: Operations successful**, type `reagentc /boottore`.

- 5 Restart the server. From the **Open Command** windows type `shutdown -x -t 0`.
- 6 When the server restarts in the **Windows Recovery Environment**, click **Troubleshoot**.



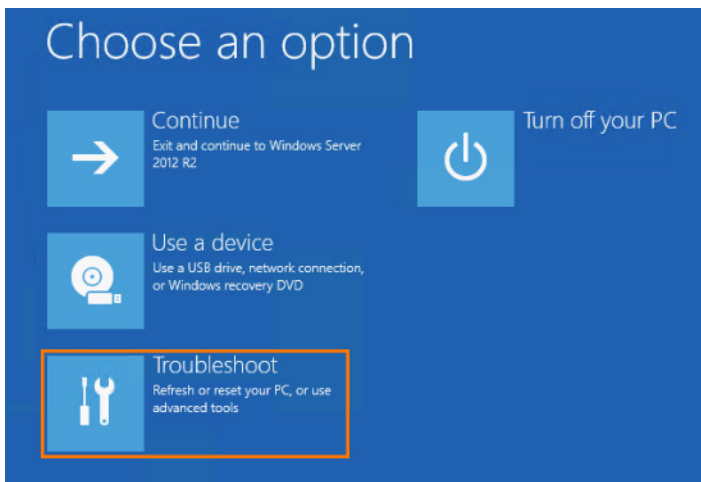


Figure 98. Windows Recovery Environment menu

- 7 On the **Troubleshoot** menu, click **Advanced options**.

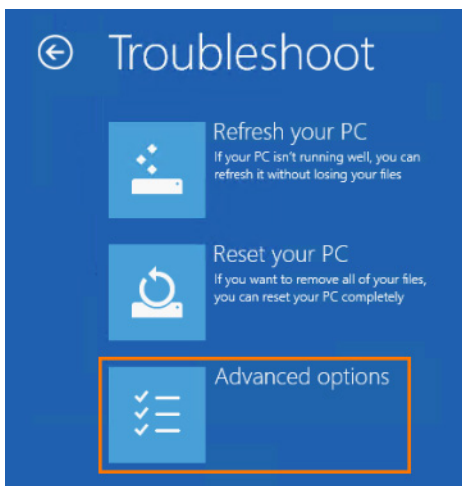
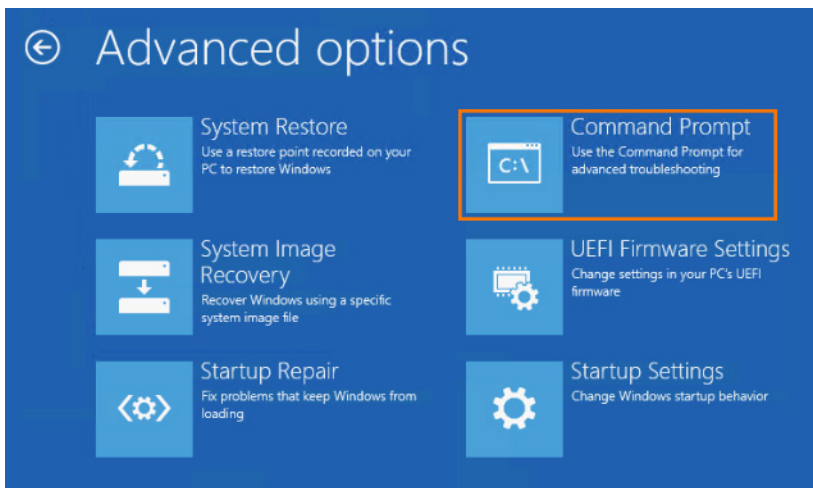


Figure 99. Troubleshoot advanced

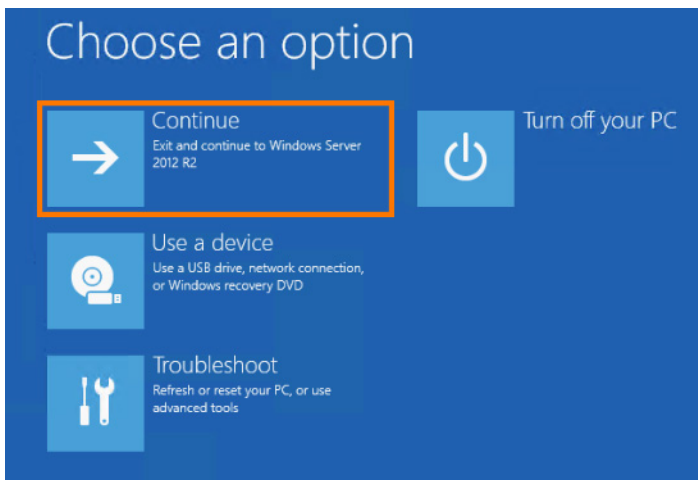
- 8 In **Advanced options**, click **Command Prompt**.



**Figure 100. Advanced options**

- 9 When a system command prompt is displayed, run the following commands:
 

```
del c:\hostos.vhdx
copy c:\recovery.vhdx c:\hostos.vhdx
del c:\vhd\console.vhdx
copy c:\vhd\console\recovery.vhdx c:\vhd\console.vhdx
```
- 10 Close the command prompt by typing **Exit**.
- 11 On the **Windows Recovery Environment** main menu, click **Continue**.



**Figure 101. Troubleshoot options**

The server restarts and completes factory first-boot automation.

**⚠ CAUTION: After completing this factory reset process, wait for at least 30 minutes before proceeding to the next step.**

- 12 The nodes require one final step. From the **iDRAC Virtual Console**, select **Power > Graceful Shutdown**. This command powers off the compute hosts. Later in the factory reset process you follow the power-on procedures for Dell Hybrid Cloud System for Microsoft, as described in [Starting up the stamp](#).

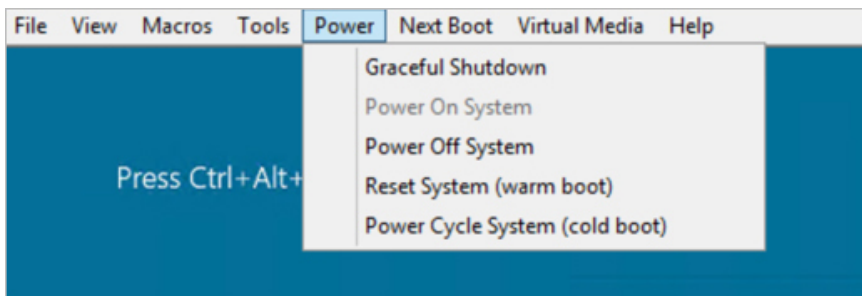


Figure 102. iDRAC Graceful Shutdown

## Clean up Active Directory and DNS records

If you want to redeploy a Dell Hybrid Cloud System for Microsoft stamp with the same customer prefix, you must remove stale objects left over from the previous deployment from your Active Directory and DNS databases.

- 1 On a domain member server or workstation with Active Directory management tools installed, open **Active Directory Users and Computers**.
- 2 Remove the organizational unit (OU) and all child objects created by the Dell Hybrid Cloud System for Microsoft deployment. The object location depends on the OU path and customer prefix that was provided during initial deployment.
- 3 Open **DNS Manager** or another DNS management tool, and remove all A-records with a name that starts with your Dell Hybrid Cloud System for Microsoft customer prefix.

## Clean up artifacts created by Azure Site Recovery

If you are using Azure Site Recovery to protect your Dell Hybrid Cloud System for Microsoft deployment, after a factory reset, the VMM server and any Infrastructure as a Service (IaaS) VMs that were created during failover are preserved in Azure.

Unless you want to recover the VHDs for the VMs and use those VHDs to recreate the VMs, you can clean up the Azure artifacts by deleting the current ASR settings on the VMM server and any IaaS VMs that were created during failover.

You might also want to delete the vault and the associated Azure storage account from the previous deployment. If you use a new customer prefix, during re-deployment, a new recovery services vault and a new storage account are created in Azure using the new prefix and the new deployment GUID.

**IMPORTANT:** It is impossible to recover any server or service after you delete it from Azure. When you delete a storage account, all content and resources for that account are permanently deleted. Before you perform these procedures, make sure you move any VMs, VHDs, or other resources that you want available later to another private, hosted, or public cloud. If you plan to use the VHDs recovered from the previous VMs to recreate new VMs, move those VHDs to a storage location outside the VMM cloud before you perform these procedures.

If you want to clean up the Azure artifacts from the previous Dell Hybrid Cloud System for Microsoft deployment, perform the applicable steps:

- Delete the VMM server
- Delete the IaaS VMs created during failover if needed
- Delete the old vault (optional)
- Delete the storage account for the old deployment (optional).

**NOTE:** In these procedures, *<Prefix>* indicates the customer prefix that was used for the stamp.

## Delete the VMM server

First, delete the VMM server from Azure Site Recovery:

- 1 Sign in to the Azure portal, at <https://portal.azure.com>, and select the appropriate subscription.
- 2 Under **Recovery Services vaults**, click the name of the vault for the Dell Hybrid Cloud System for Microsoft deployment (look for `<Prefix>-<DeploymentGUID>` or `cps-<DeploymentGUID>`) to open the vault dashboard.
- 3 In **Settings**, under **Management Servers**, click **Site Recovery servers**.
- 4 Click the VMM server (`<Prefix>VMM01`) that you want to delete. Click **Delete**, and then click **OK** to confirm.

## Delete the IaaS VMs from failover if needed

If any VM from the Dell Hybrid Cloud System for Microsoft deployment has failed over to Azure, you can delete the corresponding Azure Infrastructure as a Service (IaaS) VMs that were created during the failover.

To delete an IaaS virtual machine:

- 1 In the Azure portal (at <https://portal.azure.com>), open **Virtual Machines**.
- 2 Click the VM that you want to delete.
- 3 Click **Delete**, and then click **OK** to confirm.

## Optionally delete the vault and the associated storage account

If you plan to re-deploy the Dell Hybrid Cloud System for Microsoft stamp with a new customer prefix, you might want to delete the old recovery services vault and the old storage account associated with the vault. During re-deployment, a new recovery services vault and a new storage account are created using the new customer prefix and the deployment GUID.

### Delete the old vault (optional)

**⚠ WARNING: All deletions are permanent. It is not possible to retrieve any server or service that you delete. If you want to save any server or service, be sure to back it up outside Azure before you delete it from the vault.**

- 1 In the Azure portal, under **Recovery Services vaults**, click the vault that you want to delete. Look for the name `<Prefix>-<DeploymentGUID>` or `cps-<DeploymentGUID>` for the vault you are deleting.
- 2 In the vault dashboard, click **Delete**, and then click **Yes** to confirm the deletion.

**📌 NOTE: You can only delete a recovery vault if no objects are registered to the vault.**

### Delete the storage account for the old deployment (optional)

**⚠ WARNING: It is not possible to restore a storage account or retrieve any of the content that it contained after deletion. Be sure to back up anything that you want to save before you delete the storage account.**

- 1 Open **Storage accounts** in the Azure portal.  
To locate, click **Browse**, and then type `storage` in the search filter box.
- 2 Select the storage account (look for `<Prefix><PartialDeploymentGUID>` or `cps<PartialDeploymentGUID>`), click **Delete**, and then confirm the deletion.

**📌 NOTE: The naming convention for the storage account varies based on the update version of the Dell Hybrid Cloud System for Microsoft stamp when Azure onboarding was performed. For more information, see the Release Notes.**

# Appendix C: Retrieving cluster names, host names, and IP addresses

You can use the following Windows PowerShell commands to retrieve cluster and host names, and IP addresses for the clusters, hosts, and infrastructure VMs.

Run the commands in an elevated Windows PowerShell session on the Console VM.

Topics:

- [Get cluster names](#)
- [Get the cluster IP addresses](#)
- [Get host names and IP addresses for cluster hosts](#)
- [Get infrastructure VM names and addresses](#)

## Get cluster names

### Syntax

```
Get-Cluster -Name <StampPrefix>*
```

### Example

```
Get-Cluster -Name S54*
```

## Get the cluster IP addresses

### Example 1: Compute clusters

#### Syntax

```
Get-Cluster -Name <ComputeClusterName> | Get-ClusterResource "Cluster IP Address" | Get-ClusterParameter -Name Address
```

#### Example

```
Get-Cluster -Name S54CCL | Get-ClusterResource "Cluster IP Address" | Get-ClusterParameter -Name Address
```

### Example 2: File server clusters

#### Syntax

```
Get-Cluster -Name <FileServerClusterName> | Get-ClusterResource "Cluster IP Address" | Get-ClusterParameter -Name Address
```

#### Example

```
Get-Cluster -Name S54SCL | Get-ClusterResource "Cluster IP Address" | Get-ClusterParameter -Name Address
```

## Example 3: SQL Server clusters

#### Syntax

```
Get-Cluster -Name <SQLServerClusterName> | Get-ClusterResource "Cluster IP Address" | Get-ClusterParameter -Name Address
```

#### Example

```
Get-Cluster -Name S54SQLCL | Get-ClusterResource "Cluster IP Address" | Get-ClusterParameter -Name Address
```

## Get host names and IP addresses for cluster hosts

### Compute cluster host

#### Syntax

```
Get-ClusterNetworkInterface -Cluster <ComputeClusterName> | Format-Table -Property Node, Name, IPv4Addresses, Ipv6Addresses
```

#### Example

```
Get-ClusterNetworkInterface -Cluster S54CCL | Format-Table Node, Name, IPv4Addresses, Ipv6Addresses
```

### File server cluster

#### Syntax

```
Get-ClusterNetworkInterface -Cluster <FileServerClusterName> | Format-Table -Property Node, Name, IPv4Addresses, Ipv6Addresses
```

#### Example

```
Get-ClusterNetworkInterface -Cluster S54SCL | Format-Table -Property Node, Name, IPv4Addresses, Ipv6Addresses
```

### SQL Server cluster

#### Syntax

```
Get-ClusterNetworkInterface -Cluster <SQLServerClusterName> | Format-Table -Property Node, Name, IPv4Addresses, Ipv6Addresses
```

### Example

```
Get-ClusterNetworkInterface -Cluster S54SQLCL | Format-Table -Property Node, Name, IPv4Addresses, Ipv6Addresses
```

## Get infrastructure VM names and addresses

### Syntax

```
Get-SCStaticIPAddressPool -Name "Management_Pool" | Get-SCIPAddress | Format-Table -Property Description,Address
```

# Appendix D: Ports and protocols

The following table defines Dell Hybrid Cloud System for Microsoft protocol and port number mappings:

**IMPORTANT: Disjointed namespaces:**

- **Your domain name must be the same as the DNS zone in which your DHCS stamp resides.** For example, if your domain name is `mycompany.local`, and you are using a DNS zone other than `mycompany.local`, you have a disjointed namespace. **Dell EMC has only validated and tested contiguous namespace use case with identical domain name and the DNS zone.**
- **Your NetBIOS name for the domain must be the same as the prefix of your FQDN.** For example, if your FQDN is `mycompany.local`, and you are using a NetBIOS name of anything other than `mycompany`, you have a disjointed namespace. **Dell EMC has only validated and tested contiguous namespace where the NetBIOS name is set to the same name as the FQDN prefix. In the above example, the NetBIOS name would be “mycompany.”**

**Table 42. Protocol and port number mappings**

| Source                                | Target                                          | Protocol      | Port    | Comment                         |
|---------------------------------------|-------------------------------------------------|---------------|---------|---------------------------------|
| Local Subnet                          | All SQL VMs                                     | Service-based | MSSQL*  | Services named MSSQL*           |
|                                       |                                                 | Service-based | SQL*    | Services named SQL*             |
|                                       |                                                 | Service-based | MSOLAP* | Services named MSOLAP*          |
|                                       |                                                 | TCP           | 80      | HTTP                            |
|                                       |                                                 | TCP           | 443     | HTTPS                           |
|                                       |                                                 | TCP           | 1433    | Standard SQL listener           |
|                                       |                                                 | TCP           | 1434    | Standard Admin Connection       |
|                                       |                                                 | TCP           | 4022    | Standard SQL Service Broker     |
|                                       |                                                 | TCP           | 135     | Transact SQL/RPC                |
|                                       |                                                 | TCP           | 2382    | SQL Browser                     |
|                                       |                                                 | TCP           | 2383    | Default Analysis Services       |
|                                       |                                                 | UDP           | 1434    | SQL Browser Query               |
|                                       |                                                 | Multicast UDP |         | SQL Browser server enumerations |
| WSUS (on <b>&lt;Prefix&gt;VMM01</b> ) | Any                                             | TCP           | 80      | WSUS Updates (HTTP)             |
|                                       |                                                 | TCP           | 443     | WSUS Updates (HTTPS)            |
| Any                                   | SMA Web Endpoint ( <b>&lt;Prefix&gt;APA01</b> ) | TCP           | 9090    |                                 |
|                                       |                                                 | TCP/UDP       | 389     | LDAP                            |
|                                       |                                                 | TCP           | 636     | LDAP (SSL)                      |
|                                       |                                                 | TCP           | 3268    | Global Catalog                  |



| Source | Target                                   | Protocol | Port        | Comment                                                       |
|--------|------------------------------------------|----------|-------------|---------------------------------------------------------------|
|        |                                          | TCP      | 3269        | Global Catalog (SSL)                                          |
|        |                                          | TCP/UDP  | 88          | Kerberos                                                      |
|        |                                          | TCP/UDP  | 53          | DNS                                                           |
|        |                                          | TCP/UDP  | 445         | SMB, CIFS, SMB2, DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc |
|        |                                          | TCP      | 135         | RPC, EPM                                                      |
|        |                                          | TCP      | 1025:5000   | RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS (2003)          |
|        |                                          | TCP      | 49152:65535 | RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS (2008)          |
|        |                                          | TCP      | 5722        | RPC, DFSR (SYSVOL)                                            |
|        |                                          | UDP      | 123         | NTP                                                           |
|        |                                          | TCP/UDP  | 464         | Kerberos change/set password                                  |
|        |                                          | UDP      | 1025:5000   | DCOM, RPC, EPM (2003)                                         |
|        |                                          | UDP      | 49152:65535 | DCOM, RPC, EPM (2008)                                         |
|        |                                          | UDP      | 138         | DFSN, NetLogon, NetBIOS Datagram Service                      |
|        |                                          | TCP      | 9389        | ADWS (Active Directory Web Service)                           |
|        |                                          | UDP      | 137         | NetLogon, NetBIOS Name Resolution                             |
|        |                                          | TCP      | 139         | DSFN, NetBIOS Session Service, NetLogon                       |
| Any    | Windows Azure Pack admin (<Prefix>APA01) | TCP      | 30004       | AdminAPI                                                      |
|        |                                          | TCP      | 30018       | WebAppGallery                                                 |
|        |                                          | TCP      | 30024       | UsageCollector                                                |
|        |                                          | TCP      | 30091       | AdminSite                                                     |
|        |                                          | TCP      | 30020       | Monitoring                                                    |
|        |                                          | TCP      | 30022       | Usage                                                         |
|        |                                          | TCP      | 30005       | TenantAPI                                                     |
|        |                                          | TCP      | 30072       | WindowsAuthSite                                               |

| Source             | Target                                    | Protocol | Port           | Comment                                  |
|--------------------|-------------------------------------------|----------|----------------|------------------------------------------|
| Any                | Windows Azure Pack public (<Prefix>APT01) | TCP      | 30006          | TenantPublicAPI                          |
|                    |                                           | TCP      | 30081          | TenantSite                               |
|                    |                                           | TCP      | 30071          | AuthSite                                 |
| Local subnets      | Any                                       | UDP      | 137:138        | Allow name/share resolution              |
|                    |                                           | TCP      | 139            | Allow name/share resolution              |
| Any                | Console VM                                | TCP      | 3389           | Remote Desktop                           |
| All hosts and VMs  | Internet                                  | TCP      | 80:443         | Azure services                           |
| Local subnets      | Operations Manager (<Prefix>OM01)         | TCP      | 5723           | Operations Manager agent communication   |
|                    |                                           | TCP      | 5724           | Operations Manager console communication |
| Local subnets      | All hosts and SQL Server VMs              | TCP      | 135:1024-65535 | DPM agent communication                  |
| Management subnets | Local subnets                             | TCP/UDP  | 5985           | WS-Management                            |
| All iDRACs         | Local subnets                             | TCP      | 5900:5901      | iDRAC Console and Virtual Console        |