Contents

What is Service Provider Foundation?

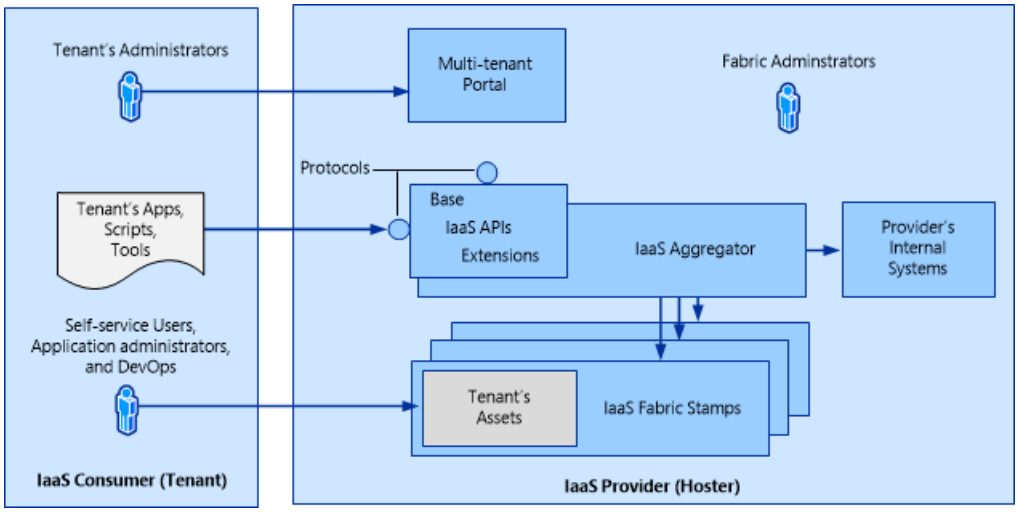
4/24/2019 • 6 minutes to read

System Center – Virtual Machine Manager (VMM), provides all the resources needed to build, maintain, and monitor a cloud infrastructure. However, service providers and large enterprises need additional features to support multiple tenants, integrate infrastructures with sophisticated web-based self-service portals, and distribute management workloads across multiple datacenters.

System Center - Service Provider Foundation (SPF), bundled with System Center Orchestrator, provides this functionality with an extensible Open Data Protocol API over a Representational State Transfer (REST) web service that interacts with VMM.

SPF can be used by service providers to offer infrastructure as a service (IaaS) to their clients. If a service provider has a frontend portal for clients, client can make requests to the hosting provider resources without leaving the portal. Cloud resources provided by VMM can be managed using standard management interfaces from supported devices anywhere.

The following graphic shows how SPF works.



SPF services

SPF provides a number of services:

- **Admin web service**: Provides servers, tenants, and stamps for Service Provider Foundation.
- **VMM service**: Provides access to VMM capabilities
- **Provider service**: Used by Windows Azure Pack

Admin web service

- Hosting service providers use the Admin web service to create and manage tenants, user roles, servers, stamps, and other administrative objects.
- You can access the Admin web service by using the URL
  `**https://server:8090/SC2016/Admin/Microsoft.Management.Odata.svc**`
- The following credentials are required

CREDENTIAL	REQUIREMENT
Admin application pool identity in IIS	Must be a member of the Admin groups and SPF_Admin group.
Admin group in Computer Management	Must include the credential for the Admin application pool identity
SPF_Admin group in Computer Management	Must include a local user who is a member of the Admin group, and the credential for the Admin application pool identity.

VMM web service

The VMM web service invokes VMM to perform requested operations, such as creating virtual machines, virtual networks, user role definitions, and other fabric for the cloud. This service coordinates the changes among the participants and provides the following dynamic capabilities:

- Portal applications and other clients detect changes that SPF and VMM made.
- VMM shows changes that portal applications, other clients, and Service Provider Foundation made.
- Service Provider Foundation reflects all changes that the participants made.

You can use the T:Microsoft.SystemCenter.Foundation.Cmdlet.New-SCSPFServer PowerShell cmdlet to register a VMM instance. You can access the VMM web service with the URL

```
https://server:8090/SC2016/VMM/Microsoft.Management.Odata.svc
```

CREDENTIAL	REQUIREMENT
VMM application pool identity in IIS	Must be a member of the Admin groups and SPF_VMM group.
Admin group in Computer Management	Must include the credential for the VMM application pool identity
SPF_VMM group in Computer Management	Must include a local user who is a member of the Admin group, and the credential for the VMM application pool identity.
Admin user role in VMM	Must include the credential for the VMM application pool identity, as a member of the Admin user role

Usage web service

- The Usage web service is only used by Windows Azure Pack, and third- party billing providers. The Usage web service endpoint shouldn't be accessed for other purposes to prevent data loss due to unnecessary or erroneous queries.
- The Usage web service uses registrations of instances of Operations Manager data warehouses (that VMM hosts) for collecting metrics on tenant virtual machine usage and other fabric usage. Usage data is collected for processes such as billing chargeback features.
- You can use Windows PowerShell cmdlets to register Operations Manager data warehouse connection settings in the SPF database. This registration enables SPF to aggregate usage data from the data warehouses.
- The Usage web service returns utilization data that pertains to every subscription across services.

CREDENTIAL	REQUIREMENT
Usage application pool identity in IIS	Must be a member of the Admin groups and SPF_Usage group.
Admin group in Computer Management	Must include the credential for the Usage application pool identity.
SPF_Usage group in Computer Management	Must include a local user who is a member of the Admin group, and the credential for the Usage application pool identity.
Database user dbo in the OperationsManagerDW SQL Server database (on the Operations Manager server)	The credentials of the user who installed Operations Manager are automatically used for logon to the dbo SQL Server security object. The same credentials should be used for all SPF application pool identities.

Database properties for the OperationsManagerDW SQL Server database (right-click) on the Operations Manager server.

Provider web service

Resource providers for delivering infrastructure as a service (IaaS) use the Provider web service. The Provider web service provides a Microsoft ASP.NET web API. It is not an Open Data (OData) service. The Provider web service also uses the VMM and Admin web services.

CREDENTIAL	REQUIREMENT
Provider application pool identity in IIS	Must be a member of the Admin groups and SPF_Provider, SPF_VMM, and SPF_Admin groups.
Admin group in Computer Management	Must include the credential for the Provider application pool identity
SPF_Provider group in Computer Management	Must include a local user who is a member of the Admin group, and the credential for the Provider application pool identity.

Service Management Automation web service.

You can configure events in SPF that the Service Mmnagement Automation web service will use. To do this, the web service must have credentials to access the SPF web services. Alternatively, you can use PowerShell to automate runbooks.

CREDENTIAL	REQUIREMENT
One or more SPF application pool identities, as required for automation	Must be a member of the Admin group on the server with Service Management Automation installed.

Interaction with SPF

Hosters and tenants interact with SPF as follows:

- Hosting providers use the Administration service to allocate networking bandwidth, disk space, and servers, which together represent the private cloud to tenants.
- Tenants represents a customer with asset on the hoster system. Tenants consume and manage services that the hosting provider has offered to them. Each tenant has their own administrators, applications, scripts, and other

tools.

- A hosting provider manages the resources that each tenant has available to it. The hoster has an existing frontend portal, which all tenants can use.
- Tenant services are provisioned to self-service users by tenant administrators in the form of virtual machine networks, virtual machines, virtual hardware, and cloud infrastructure.
- The hoster allocates fabric resources into a stamp. Tenant resources can be allocated to stamps in whatever manner is appropriate to the hoster. Resources may be divided across several stamps (defined collection of resources).
- SPF allows the hoster to present a seamless user experience to the tenant by aggregating the data from each stamp and allowing the tenant to use SPF APIs to access that data.
- As tenant demand increases, the hoster provides additional stamps to meet the demand.
- Each instance of VMM that SPF interacts with is known as a management stamp. SPF can interact with a maximum of five stamps.
    - A stamp is a System Center instance that supports a virtualized platform infrastructure that consists of the VMM server, hosts, VMs, and configuration settings such as service accounts and user roles. Stamps provide a logical boundary. For example, you could have a separate stamp for each site managed by a VMM server.
    - Stamps must be capable of being monitored and will include an instance of System Center Operations Manager. An Operations Manager instance can provide monitoring for multiple stamps.
- Tenant administrators can interact with the VMM fabric by configuring clouds, templates, user roles, and self-service users, among other things. A tenant administrator also has self-service user capabilities.
- Self-service users are provided with a subset of tenant resources to work with. Resource usage is controlled by quota. For example, when users deploy virtual machines or use other resources, they incur quota points up to the number of allocated available quota points. Self-service users can interact with services, templates, and VHDs to deploy and manage virtual machines.

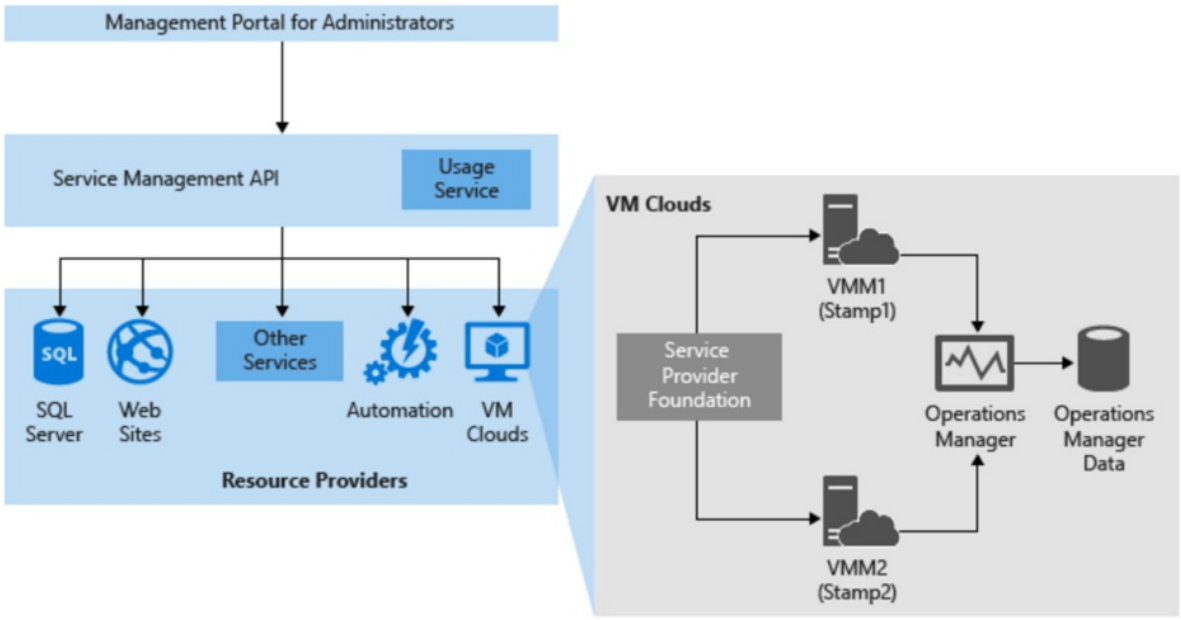
This graphic shows how SPF interacts with VMM

VMM, SPF and Windows Azure Pack

Windows Azure Pack provides an Azure-like experience and frontend for organizational clouds. Azure Pack provides a number of components, and among them, the VM cloud service. The VM cloud service with integrates with VMM to provide:

- A management portal for administrator to enable hosting or service provides to set up a VM provisioning infrastructure

- A tenant portal where tenants can sign up for the VM Clouds service, and provision VMs. Windows Azure Pack uses SPF to integrate with VMM to provide the VM Clouds service, as illustrated in the following graphic.



Next steps

Plan SPF deployment

What's new in System Center - Service Provider Foundation

3/21/2019 • 2 minutes to read

This article details the new features supported in System Center 2019 - Service Provider Foundation (SPF).

No new features are introduced with System Center 1807 - Service Provider Foundation (SPF).

This article details the new features supported in System Center 1801 - Service Provider Foundation (SPF).

Support for TLS 1.2

This release of System Center Service Provider Foundation (SPF) contains all the bug fixes shipped till the Update Rollup 2 of SPF 2016, along with added support for TLS 1.2 Protocol. For more information about how to set up, configure and run your environment to use TLS 1.2, Read this article.

This build should be used for validating the SPF integration scenarios with other System Center components included in the 1801 release.

Support for PowerShell 4.0+

Earlier versions of SPF supported PowerShell V2.0. PowerShell V2.0 did not support some scripts and users had to apply workarounds. SPF 2019 supports PowerShell V4.0 to resolve this issue.

Support for SQL 2017

SPF 2019 supports SQL 2017 for fresh installation.

Bug fixes

This release of System Center Service Provider Foundation (SPF) contains all the bug fixes shipped till the Update Rollup 2 of SPF 2016.

> **NOTE**
> No features were introduced in SPF 1807.

> **NOTE**
> The following features/feature updates were introduced in SPF 1801.

Support for TLS 1.2

This release of System Center Service Provider Foundation (SPF) contains all the bug fixes shipped till the Update Rollup 2 of SPF 2016, along with added support for TLS 1.2 Protocol. For more information about how to set up, configure and run your environment to use TLS 1.2, Read this article.

This build should be used for validating the SPF integration scenarios with other System Center components included in the 1801 release.

Next steps

- Know the fixed issues

Release notes for System Center Service Provider Foundation

3/21/2019 • 2 minutes to read

This article lists the release notes for System Center 2019 - Service Provider Foundation (SPF).

SPF 2019 release notes

This release of System Center Service Provider Foundation (SPF) contains all the bug fixes shipped till the Update Rollup 2 of SPF 2016.

The release notes for System Center 1807 - Service Provider Foundation (SPF) is applicable for System Center 1801 - Service Provider Foundation (SPF).

This article lists the release notes for System Center 1801 - Service Provider Foundation (SPF).

SPF 1801 release notes

This release of System Center Service Provider Foundation (SPF) contains all the bug fixes shipped till the Update Rollup 2 of SPF 2016.

Next steps

What's new in Service Provider Foundation

Turn off telemetry settings in Service Provider Foundation

5/16/2019 • 2 minutes to read

This article provides information about how to turn off the telemetry settings in System Center - Service Provider Foundation (SPF).

By default, SPF sends diagnostic and connectivity data to Microsoft. Microsoft uses this data to provide and improve the quality, security, and integrity of Microsoft products and services.

Administrators can turn off this feature at any point of time.

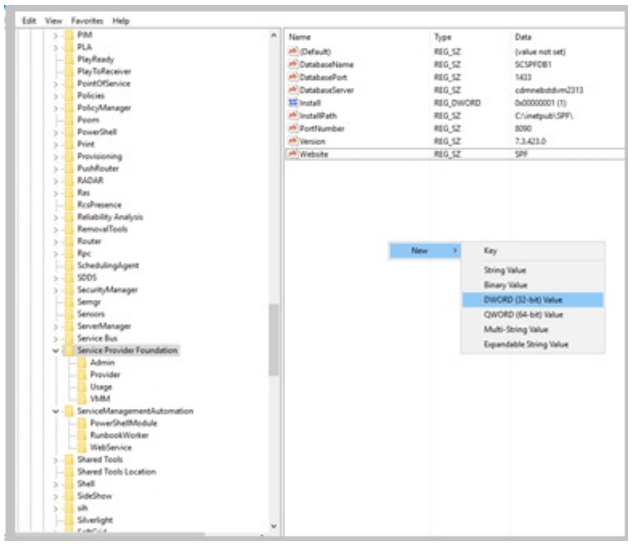
> **NOTE**
> Microsoft does not collect any personal data from the customers. We only listen to events that would help diagnostics in SPF. Learn more.

Turn off telemetry in SPF

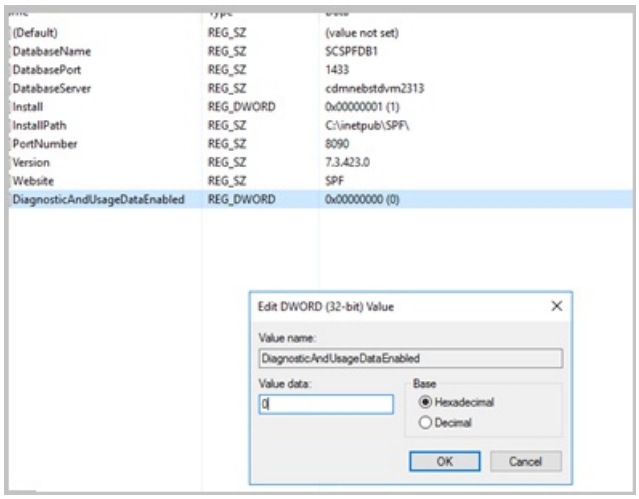
Use the following procedure:

1. On the SPF server, Set the value of the "DiagnosticAndUsageDataEnabled" registry subkey under *HKEY_LOCAL_MACHINE\Software\Microsoft\Service Provider Foundation* to 0. If the registry key is not present, then create the key with the name *DiagnosticAndUsageDataEnabled* and set the value to 0.

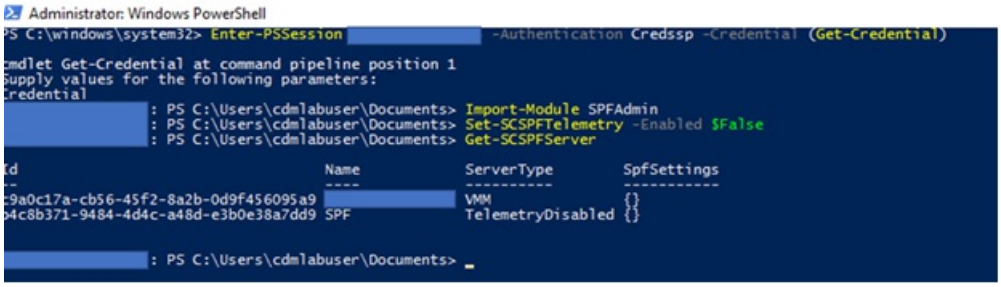
   - To create a new Registry Key, under HKEY_LOCAL_MACHINE\Software\Microsoft\Service Provider Foundation, right-click, and select **New** > **DWORD (32-bit) Value** as shown below:

   - Enter the name of the key as *DiagnosticAndUsageDataEnabled*.
   - Once the key appears in the list of keys double-click on the key and enter 0 in the *Value data* field as shown below:



2. Use the *Set-SCSpfTelemetry* command and set the telemetry option as shown in the following image:



Telemetry data collected

DATA RELATED TO	DATA COLLECTED
Installation and other configuration information	SPF version ID used for correlation with other System Center products Version and language settings of the Operating System Processor and memory Details of the system Setup errors If Silent Mode is enabled Setup failure and (or) cancellation Whether prerequisites check is run again SQL version and whether Always On, Clustered and Remote are being used Information regarding the missing prerequisite, if any.
Usage	VMM endpoint being accessed Resources used. For example, virtual machine, virtual network. Type of operation – create, update, delete

Next steps

Manage run books

Plan SPF deployment

12/6/2018 • 4 minutes to read

This article helps you make sure you have prerequisites and planning steps in place, before you deploy System Center - Service Provider Foundation (SPF).

Deployment prerequisites

Deployment requirements for SPF include:

- Make sure you have the minimum hardware and software requirements on the SPF server.
- The SPF server needs SQL Server for its database. The SQL Server database can be local, or on a remote server and should have at least 5 GB of storage. When you install SPF you need to specify the server name and port number. Learn more about supported SQL Server versions.
- The VMM console should be installed on the SPF server. SPF can also run on the same server as the VMM management server. VMM must be deployed in your infrastructure.
- If you want to use usage metering to manage tenant costs, you need a System Center Operations Manager server, and a Data Warehouse server, running Windows 2012 R2 or later.
- The following Server Manager features should be installed on the SPF server:
  - Role: Web Server (IIS) server. Include the following services:
    - Basic Authentication
    - Windows Authentication
    - Application Deployment ASP.NET 4.5
    - Application Development ISAPI Extensions
    - Application Deployment ISAPI FiltersAzure
    - IIS Management Scripts and Tools Role Service
  - Feature: Management OData IIS Extension
  - Feature: .NET Framework 4.5 features, WCF Services, HTTP Activation
- Install the following web services:
  - WCF Data Services 5.0 for OData V3
  - ASP.NET MVC 4
- You need an SSL server certificate. You can generate a test certificate automatically during setup, but we recommend you use that for testing purposes only, and obtain a certificate from a CA for your production environment.
- A side-by-side installation of different SPF versions on the same server isn't supported.
- You can install on a VM.
- Make sure that you have a domain user account with administrative privileges on the computers on which you want to install Service Provider Foundation.

Administrator roles

Administrator roles Here's what you need:

- SQL Server administrator: A DBA role with full administrator rights on the SQL Server instance used by SPF. The administrator should be able to grant permissions to create databases, and to grant those permissions to the SPF administrator.
- SPF administrator: The SPF administration account should be a local administrator on the server on which you

install SPF.

- Application pool user: This IIS role should have full administrator permissions in VMM, and permissions to create, read, update, and delete on the SPF database. For portal applications, these operations can be restricted to specific tables.

Plan security

SPF implements Windows and IIS security features. Requirements include:

- Domain credentials must be used.
- SPF relies on IIS for user authentication. Only SSL (HTTPS) requests are accepted from provider endpoints, using default port 8090. Typically, the request should have the security context of the logged on user to make the request.
- When the setup wizard installs a web service, it creates a local security group on the computer, to run the service. You can specify users or groups with access to each web service and assign them to this local group. SPF checks that users sending requests belong to the appropriate local security group.
- The setup wizard creates application domain pools in IIS for each web service. You can specify the Network Service account, or an account that belongs to the security group. The wizard creates the following security group application pools: SPF_Admin: Admin
  - SPF_VMM: VMM
  - SPF_Provider: Provider
  - SPF_Usage: Usage

Plan capacity

- Database storage: 5 GB is sufficient even for large SPF databases.
- Web service: By default, SPF supports up to 1000 concurrent requests for its web services. We recommend this be a lower number in a production environment. You can change this configuration by specifying the value for the MaxRequestsPerTimeSlot key in the C:\inetpub\SPF\web.config file.
- Hardware recommendations: The following server scenarios each pertain to the recommendations listed in the following table.
  - Virtual Machine Manager (VMM) with or without SQL Server
  - Service Provider Foundation with or without SQL Server

5000 OR LESS VMS	5000-12,000 VMS	12,000 - 25,000 VMS
4 processor cores, 8 GB RAM	8 processor cores, 8 GB RAM	16 processor cores, 8 GB RAM. Recommended for computers running VMM with or without SQL Server.

Plan database

There are two database scenario configurations:

- Install SPF and connect to an existing database. In this scenario the SPF administrator must verify that the permissions for the database were granted by the database administrator as follows:
  - Alter: Create tables
  - Connect with Grant: Connect to existing database
  - Select with Grant, Update with Grant, Delete with Grant, Insert with Grant: Grant permissions to application pool users

- Alter all logins: Create SQL Server logins for application pool users.

- Create a new database. In this scenario the database administrator must create the database (SCSPFDB) and then SPF administrator installs SPF, and has permissions to configure the database as needed. For example to add tables. SPF administrators must create SPF Application Pool in Internet Information Services (IIS) and create a database user for an Application Pool User with the following permissions:
  - Connect: Connect to the SPF database
  - Select, Update, Delete, Insert: Perform basic operations
  - Create the SQL Server logon for Application Pool User with default database set to SCSPFDB.: To log on to SQL Server and access the database.

Next steps

Deploy SPF

System requirements for System Center Service Provider Foundation

3/14/2019 • 2 minutes to read

This article details the system requirements for System Center 2019 - Service Provider Foundation (SPF).

System requirements for System Center 2019 - Service Provider Foundation

The following sections describe the hardware and software requirements for System Center 2019 - Service Provider Foundation (SPF).

Hardware

HARDWARE	SUPPORTED
Processor (minimum)	2.1 GHx dual core CPU or faster
Processor (recommended)	2.1 GHx dual core CPU or faster
RAM (minimum)	8 GB
RAM (recommended)	16 GB

Server operating system

OPERATING SYSTEM	SUPPORTED
Windows Server 2019r	Y
Windows Server 2019 (with desktop experience)	Y
Windows Server 2016	Y
Windows Server 2016 (with desktop experience)	Y

SQL Server

> **NOTE**
> For the supported versions of SQL, use the service packs that are currently in support by Microsoft.

SQL VERSION	SUPPORTED
SQL Server 2017	Y

SQL VERSION	SUPPORTED
SQL Server 2016 and SPs as detailed here	Y

Installation components

These components should be installed on the server, before you install VMM.

INSTALLATION	SUPPORTED
PowerShell	PowerShell 4.0, 5.0
.NET	4.5.2, 4.6

System requirements for SPF 1801 are also applicable for SPF 1807, there are no changes. Learn about the system requirements.

This article details the system requirements for System Center 1801 - Service Provider Foundation (SPF).

This article details the system requirements for System Center 2016 - Service Provider Foundation (SPF).

System requirements for System Center 1801 - Service Provider Foundation

The following sections describe the hardware and software requirements for System Center 1801 - Service Provider Foundation (SPF).

Hardware

HARDWARE	SUPPORTED
Processor (minimum)	2.1 GHx dual core CPU or faster
Processor (recommended)	2.1 GHx dual core CPU or faster
RAM (minimum)	8 GB
RAM (recommended)	16 GB

Server operating system

OPERATING SYSTEM	SUPPORTED
Windows Server 2012 Standard/Datacenter	N
Windows Server 2012 R2 Standard/Datacenter	N
Windows Server 2016	Y
Windows Server 2016 (with desktop experience)	Y
Windows Server 2016 Nano	N

SQL Server

> **NOTE**
> For the supported versions of SQL, use the service packs that are currently in support by Microsoft.

SQL VERSION	SUPPORTED
SQL Server 2008	N
SQL Server 2012 and SPs as detailed here	Y
SQL Server 2014 and SPs as detailed here	Y
SQL Server 2016 and SPs as detailed here	Y

Installation components

These components should be installed on the server, before you install VMM.

INSTALLATION	SUPPORTED
PowerShell	PowerShell 4.0, 5.0
.NET	4.5.2, 4.6

System requirements for Service Provider Foundation 2016

The following sections describe the hardware and software requirements for System Center 2016 - Service Provider Foundation (SPF).

Hardware

HARDWARE	SUPPORTED
Processor (minimum)	2.1 GHx dual core CPU or faster
Processor (recommended)	2.1 GHx dual core CPU or faster
RAM (minimum)	8 GB
RAM (recommended)	16 GB

Server operating system

OPERATING SYSTEM	SUPPORTED
Windows Server 2012 Standard/Datacenter	N
Windows Server 2012 R2 Standard/Datacenter	N

OPERATING SYSTEM	SUPPORTED
Windows Server 2016	Y
Windows Server 2016 (with desktop experience)	Y
Windows Server 2016 Nano	N

SQL Server

> **NOTE**
> For the supported versions of SQL, use the service packs that are currently in support by Microsoft.

SQL VERSION	SUPPORTED
SQL Server 2008	N
SQL Server 2012 and SPs as detailed here	Y
SQL Server 2014 and SPs as detailed here	Y
SQL Server 2016 and SPs as detailed here	Y

Installation components

These components should be installed on the server, before you install VMM.

INSTALLATION	SUPPORTED
PowerShell	PowerShell 4.0, 5.0
.NET	4.5.2, 4.6

Next steps

Deploy Service Provider Foundation.

Upgrade System Center Service Provider Foundation

3/14/2019 • 10 minutes to read

You must have System Center - Service Provider Foundation 1801 installed to apply the 2019 update.

Upgrade to System Center 2019 - Service Provider Foundation

The following sections describe the procedures required to upgrade from SPF 2016/1801/1807 to SPF 2019.

Prerequisites

- SPF:
  - If you are using SPF 2016, install update rollup 2 or later.
- VMM:
  - If you are using VMM 2016, install update rollup 6 or later.
- Windows Azure Pack - Install update rollup 12, or later.
- VMM management console - The machine running the VMM 2016/1801/1807 management console should have the latest VMM updates installed.

Assumptions

The upgrade instructions in this article assume the following scenario:

- SPF and VMM are running on System Center 2016/1801/1807
- We highly recommend that you reuse the current SPF server name to simplify the seamless integration into your existing Windows Azure Pack deployment.
- The VMM console is installed on a separate computer.
- The upgrade uses the existing SPF server name.
- These upgrade instructions assume that the VMM 2019 upgrade has already been completed, and that the necessary backups of the current Windows Azure Pack environment have been performed.

Upgrade order

Here's the recommended upgrade order for the above scenario:

1. Update the VMM console to 2019. If required, update the VMM server to 2019.
2. Update SPF to 2019.

Before you start

1. Make sure Windows Azure Pack, SPF, and VMM are all running the required updates.
2. We recommend that you shut down VMM and Windows Azure Pack servers, removing all database activity.
3. Verify SPF system requirements. Note that SPF must run on Windows Server 2016/2019 - Core or Desktop experience.
4. Verify VMM console requirements.

Run the SPF upgrade

Prepare the SPF 2019 computer on which you want to run the upgrade.

1. Create a new server running Windows Server 2019, on which you want to install SPF 2019. You can also use a Virtual Machine (VM).
2. In our example, we'll create a machine call **SERVER-SPF-UPGRADE**.
3. Install the prerequisites on the new VM, as follows:
   - Install SQL ODBC Drivers.
   - Install SQL Native Client
   - Install SQL Server command line utilities.
   - Install SQL Server CLR types.
   - Install IIS with the following features: PowerShell: Install-WindowsFeature Web-Server, Web-WebServer, Web-Common-Http, Web-Default-Doc, Web-Dir-Browsing, Web-Http-Errors, Web-Static-Content, Web-Health, Web-Http-Logging, Web-Request-Monitor, Web-Http-Tracing, Web-Performance, Web-Stat-Compression, Web-Security, Web-Filtering, Web-Basic-Auth, Web-Windows-Auth, Web-App-Dev, Web-Net-Ext45, Web-Asp-Net45, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Mgmt-Tools, Web-Mgmt-Console, Web-Scripting-Tools, NET-Framework-45-ASPNET, NET-WCF-HTTP-Activation45, ManagementOdata, WAS, WAS-Process-Model, WAS-Config-APIs.
   - Install WCF Data Services 5.0 for OData V3.
   - Install ASP.NET MVC 4.
4. Install the latest Windows updates on the VM.
5. Restart the VM to make sure there are no pending reboots.

> **NOTE**
> Don't join the VM to a domain.

Remove SPF 2016/1801/1807

1. Uninstall the VMM admin console on the SPF machine.
2. Uninstall the SPF Web Component on the SPF machine.
3. Rename the machine. For example, from **SERVER-SPF-01** to **SERVER-SPF-OLD**.

Set up the SPF 2019 computer

1. Rename the VM you set up. Use the original name of the SPF computer. So change the VM name from **SERVER-SPF-UPGRADE** to **SERVER-SPF-01**.
2. Join the VM to the domain.
3. Install the VMM console.For a core installation you can install from the command line, or set up from the user interface and change to Core later.
4. Install SPF 2019, using the existing SQL Server database name during setup.

Post-upgrade tasks

1. SPF needs a server certificate for website binding. You can use the self-signed certificate generated during setup, but we don't recommend this for a production environment.
2. If you do use a self-signed certificate:
   - It should be used only for testing purposes.
   - The FQDN should be specified for the certification path instead of "localhost".
   - It should be located in the personal or webhosting store.

Test Windows Azure Pack

Test everything's working as follows:

1. Start VMM 2019.

2. In the Windows Azure Pack Admin portal, check in this order: 1) VMs; 2) Gallery items; 3) Templates; 4) SPF configuration settings. Make sure everything's working as expected.
3. In the Windows Azure Pack Tenant portal, check in this order: 1) Deployment settings; 2) VMs; 3) Plans; 4) Deployment options. Make sure everything's working as expected.

You must have System Center - Service Provider Foundation 1801 installed to apply the 1807 update.

This article provides the upgrade information for System Center 1801 - Service Provider Foundation (SPF).

Upgrade to System Center 1801 - Service Provider Foundation

The following sections describe the procedures required to upgrade from System Center 2012 R2 SPF or System Center 2016 SPF to SPF 1801.

Prerequisites

- SPF:
  - On System Center 2012 R2 install update rollup 12 or later, in order to upgrade to 1801.
  - On System Center 2016 install update rollup 2 or later, in order to upgrade to 1801.
- VMM:
  - On System Center 2012 R2 install update rollup 12 or later, in order to upgrade to 1801.
  - On System Center 2016 install update rollup 2 or later, in order to upgrade to 1801.
- Windows Azure Pack - Install update rollup 12, or later.
- VMM management console - The machine running the VMM 2012 R2 or 2016 management console should have the latest VMM updates installed.

Assumptions

The upgrade instructions in this article assume the following scenario:

- SPF and VMM are running on System Center 2016
- We highly recommend that you reuse the current SPF server name to simplify the seamless integration into your existing Windows Azure Pack deployment.
- The VMM console is installed on a separate computer.
- The upgrade uses the existing SPF server name.
- These upgrade instructions assume that the VMM 1810 upgrade has already been completed, and that the necessary backups of the current Windows Azure Pack environment have been performed.

Upgrade order

Here's the recommended upgrade order for the above scenario:

1. Update the VMM console to 1801. If required, update the VMM server to 1801.
2. Update SPF to 1801.

Before you start

1. Make sure Windows Azure Pack, SPF, and VMM are all running the required updates.
2. We recommend that you shut down VMM and Windows Azure Pack servers, removing all database activity.
3. Verify SPF system requirements. Note that SPF must run on Windows Server 2016 - Core or Desktop experience.
4. Verify VMM console requirements.

Run the SPF upgrade

Prepare the SPF 1801 machine

1. Create a new server running Windows Server 2016, on which to install SPF 1801. You can use a VM. In our example, we'll create a machine call **SERVER-SPF-UPGRADE**.
2. Install the prerequisites on the new VM, as follows:
   - Install SQL ODBC Drivers.
   - Install SQL Native Client
   - Install SQL Server command line utilities.
   - Install SQL Server CLR types.
   - Install IIS with the following features: PowerShell: Install-WindowsFeature Web-Server, Web-WebServer, Web-Common-Http, Web-Default-Doc, Web-Dir-Browsing, Web-Http-Errors, Web-Static-Content, Web-Health, Web-Http-Logging, Web-Request-Monitor, Web-Http-Tracing, Web-Performance, Web-Stat-Compression, Web-Security, Web-Filtering, Web-Basic-Auth, Web-Windows-Auth, Web-App-Dev, Web-Net-Ext45, Web-Asp-Net45, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Mgmt-Tools, Web-Mgmt-Console, Web-Scripting-Tools, NET-Framework-45-ASPNET, NET-WCF-HTTP-Activation45, ManagementOdata, WAS, WAS-Process-Model, WAS-Config-APIs.
   - Install WCF Data Services 5.0 for OData V3.
   - Install ASP.NET MVC 4.
3. Install the latest Windows updates on the VM.
4. Restart the VM to make sure there are no pending reboots.
5. Don't join the VM to a domain.

Remove SPF 2012 R2/2016

1. Uninstall the VMM admin console on the SPF machine.
2. Uninstall the SPF Web Component on the SPF machine.
3. Rename the machine. For example, from **SERVER-SPF-01** to **SERVER-SPF-OLD**.

Set up the SPF 1801 machine

1. Rename the VM you set up to the original name of the SPF machine, so from **SERVER-SPF-UPGRADE** to **SERVER-SPF-01**.
2. Join the VM to the domain.
3. Install the VMM console.For a core installation you can install from the command line, or set up from the user interface and change to Core later.
4. Install SPF 2016, using the existing SQL Server database name during setup.

Post-upgrade tasks

1. SPF needs a server certificate for website binding. You can use the self-signed certificate generated during setup, but we don't recommend this for a production environment.
2. If you do use a self-signed certificate:
   - It should be used only for testing purposes.
   - The FQDN should be specified for the certification path instead of "localhost".
   - It should be located in the personal or webhosting store.

Test Windows Azure Pack

Test everything's working as follows:

1. Start VMM 1801.
2. In the Windows Azure Pack Admin portal, check in this order: 1) VMs; 2) Gallery items; 3) Templates; 4) SPF

configuration settings. Make sure everything's working as expected.

3. In the Windows Azure Pack Tenant portal, check in this order: 1) Deployment settings; 2) VMs; 3) Plans; 4) Deployment options. Make sure everything's working as expected.

This article provides the upgrade information for System Center 2016 - Service Provider Foundation (SPF).

Upgrade to System Center 2016 - Service Provider Foundation

The following sections provide information about how to upgrade from System Center 2012 R2 SPF to SPF 2016.

Prerequisites

- SPF 2016 requires Windows Server 2016.
- SPF should be running update rollup 9 or later, in order to upgrade to 2016.
- The VMM server should be running update rollup 9 or later, in order to upgrade to 2016.
- The VMM console machine should be running update rollup 9 or later, in order to upgrade to 2016.
- Windows Azure Pack should be running on Windows Server 2012 R2 with at least update rollup 10.

Assumptions

The upgrade instructions in this article assume the following scenario:

- SPF and VMM are running on System Center 2012 R2.
- We highly recommend that you reuse the current SPF server name to simplify the seamless integration into your existing Windows Azure Pack deployment.
- The VMM console is installed on a separate computer.
- The upgrade uses the existing SPF server name.
- These upgrade instructions assume that the VMM 2016 upgrade has already been completed, and that the necessary backups of the current Windows Azure Pack environment have been performed.

Upgrade order

Here's the recommended upgrade order for the above scenario

1. Update the VMM console to 2016. We're presuming you've already updated the VMM server to 2016. Read this article if you haven't.
2. Update SPF to 2016.

Before you start

1. Make sure Windows Azure Pack, SPF, and VMM are all running the required updates.
2. We recommend that you shut down VMM and Windows Azure Pack servers, removing all database activity.
3. Verify SPF system requirements. Note that SPF must run on Windows Server 2016 - Core or Desktop experience.
4. Verify VMM console requirements.

Run the SPF upgrade

Prepare the SPF 2016 machine

1. Create a new server running Windows Server 2016, on which to install SPF 2016. You can use a VM. In our example, we'll create a machine call **SERVER-SPF-UPGRADE**.
2. Install the prerequisites on the new VM, as follows:

- Install SQL ODBC Drivers.
- Install SQL Native Client
- Install SQL Server command line utilities
- Install SQL Server CLR types.
- Install IIS with the following features: PowerShell: Install-WindowsFeature Web-Server, Web-WebServer, Web-Common-Http, Web-Default-Doc, Web-Dir-Browsing, Web-Http-Errors, Web-Static-Content, Web-Health, Web-Http-Logging, Web-Request-Monitor, Web-Http-Tracing, Web-Performance, Web-Stat-Compression, Web-Security, Web-Filtering, Web-Basic-Auth, Web-Windows-Auth, Web-App-Dev, Web-Net-Ext45, Web-Asp-Net45, Web-ISAPI-Ext, Web-ISAPI-Filter, Web-Mgmt-Tools, Web-Mgmt-Console, Web-Scripting-Tools, NET-Framework-45-ASPNET, NET-WCF-HTTP-Activation45, ManagementOdata, WAS, WAS-Process-Model, WAS-Config-APIs.
- Install WCF Data Services 5.0 for OData V3.
- Install ASP.NET MVC 4.

3. Install the latest Windows updates on the VM.
4. Restart the VM to make sure there are no pending reboots.
5. Don't join the VM to a domain.

Remove SPF 2012 R2

1. Uninstall the VMM admin console on the SPF 2012 R2 machine.
2. Uninstall the SPF Web Component on the SPF 2012 R2 machine.
3. Rename the machine. For example, from **SERVER-SPF-01** to **SERVER-SPF-OLD**.

Set up the SPF 2016 machine

1. Rename the VM you set up to the original name of the SPF 2012 R2 machine, so from **SERVER-SPF-UPGRADE** to **SERVER-SPF-01**.
2. Join the VM to the domain.
3. Install the VMM console.For a core installation you can install from the command line, or set up from the user interface and change to Core later.
4. Install SPF 2016, using the existing SQL Server database name during setup.

Post-upgrade tasks

1. On the SPF machine, install the latest update: update rollup 2 for SPF 2016
2. SPF needs a server certificate for website binding. You can use the self-signed certificate generated during setup, but we don't recommend this for a production environment. If you do use a self-signed certificate:
   - It should be used only for testing purposes.
   - The FQDN should be specified for the certification path instead of "localhost".
   - It should be located in the personal or webhosting store.

Test Windows Azure Pack

Test everything's working as follows:

1. Start VMM 2016.
2. In the Windows Azure Pack 2012 R2 Admin portal, check in this order: 1) VMs; 2) Gallery items; 3) Templates; 4) SPF configuration settings. Make sure everything's working as expected.
3. In the Windows Azure Pack 2012 R2 Tenant portal, check in this order: 1) Deployment settings; 2) VMs; 3) Plans; 4) Deployment options. Make sure everything's working as expected.

Next steps

Manage SPF

Deploy SPF

12/6/2018 • 3 minutes to read

This article describes how to install System Center - Service Provider Foundation (SPF).

SPF is part of System Center - Orchestrator. SPF exposes an extensible OData web service that interacts with System Center Virtual Machine Manager (VMM) that enables service providers and hosters to design and implement multi-tenant self-service portals that integrate IaaS capabilities into System Center.

Before you begin

- Read the planning article, to make sure deployment prerequisites are in place.
- You can install SPF on a single server or on multiple servers.
- We recommend you install as an administrator, so that you can configure customer experience and Microsoft update settings during installation.
- Remember you'll need a SQL Server database for SPF on the same server, or on a remote server.
- Before you install, make sure to close any open programs, and check there's no restart pending.
- Side-by-side installation of different SPF versions on the same server isn't supported.
- You can install SPF on a VM.
- The credentials of the user who installs SPF are used for the login credentials for the dbo SQL Server security object for the SPF database. Use the T:Microsoft.SystemCenter.Foundation.Cmdlet.Get-SCSPFConnectionString and T:Microsoft.SystemCenter.Foundation.Cmdlet.Set-SCSPFConnectionString cmdlets to manage connections to the database.

Create a certificate

SPF needs a server certificate for website bindings. The SPF website is the endpoint for the Admin and VMM services that use REST and OData technology to communicate with clients and portal applications. You can generate and use a self-signed certificate, or use an existing/new CA certificate. We don't recommend self-signed certificates in a production environment. If you generate a self-signed certificate, note the following:

- A self-signed certificate should be used only for testing purposes.
- The FQDN should be specified for the certification path instead of "localhost".
- The self-signed certificate should be located in the personal or webhosting store.

Install SPF

1. On the server on which you want to install SPF, double-click **SetupOrchestrator.exe** on the installation media, to start the Setup Wizard.
2. In the main Setup page, click **Service Provider Foundation**.
3. In **Service Provider Foundation Setup**, click **Install**.
4. In **License Terms**, review the license agreement. If you agree with the terms, select **I have read, understood, and agree with the terms of the license agreement** > **Next**.
5. In **Prerequisites**, wait for the wizard to complete the prerequisite verification, and review the results. If any of the prerequisites are missing, install them and click **Check prerequisites** again. Then click **Next**.
6. In **Configure the database server**, specify the SQL Server computer name, or accept the default localhost. In **Port Number**, accept the default or modify the setting. Then click **Next**.
7. In **Specify a location for the SPF files**, accept or change the location for the web service files. Optionally,

change Website and port settings. The server certificate is used configure the site bindings for the SPF website in IIS. You can select to automatically generate a self-signed certificate for test purposes. Then click **Next**.

8. In **Configure the Admin web service**, specify the domain and user name of each security group or user who will use this web service, in the format: domain\user name with a semicolon to separate multiple entries.
9. Specify the account you want the application pool to use. It should be a domain account, with permissions to make changes on the server. We recommend you use a service account and not Network Service. If you do use Network Service the account must be a VMM administrator.
10. Configure the settings for the Provider, VMM, and Usage web services.
11. In **Microsoft Update**, select how you want to install updates, and click **Next**.
12. In **Installation summary**, review the settings. Click **Install** when you're ready.
13. Click **Close** when you see the "Setup is complete" message.
14. Repeat this procedure if needed. For example for a web farm.

If installation fails, refer to the log files: Microsoft Service Provider*.log", in the %SYSTEMDRIVE%%TEMP% folder.

Next steps

Manage SPF

Register the SPF endpoint in Windows Azure Pack

12/6/2018 • 2 minutes to read

For System Center - Service Provider Foundation (SPF) to provide services and connectivity for delivering IaaS in Windows Azure Pack, you need to register it.

1. On the SPF server, note the credentials used for the Admin, VMM, Usage, and Provider Application Pool identity in IIS.
2. Register the SPF endpoint with the Azure Pack management portal. After it's registered you can enable the VM Clouds service from the portal.

Manage tenants and user roles in SPF

3/14/2019 • 3 minutes to read

System Center - Service Provider Foundation (SPF) doesn't create user roles, or define their scope. To set up tenants you need a certificate public key that's used to validate claims made (or on behalf of) a tenant.

Create a certificate

If you don't have an existing CA certificate to use, you can generate a self-signed certificate. You can to export public and private keys from the certificate, and associate the public key with a tenant.

Obtain a self-signed certificate

Create a certificate using makecert.exe (Certificate Creation Tool).

1. Open a command prompt as administrator.
2. Generate the certificate by running the following command:

```
makecert -r -pe -n "cn=contoso.com" -b 07/12/2012 -e 09/23/2014 -ss My -sr CurrentUser -sp "Microsoft
RSA SChannel Cryptographic Provider" -sy 12 -sky exchange
```

3. This command puts the certificate in the Current User Certificate Store. To access it, on **Start** screen, type **certmgr.msc** and then in the **Apps** results click **certmgr.msc**. In the **certmgr** window, click **Certificates - Current User** > **Personal** > **Certificates** folder.

Export the public key

1. Right-click the certificate > **All Tasks** > **Export**.
2. In **Export Private Key**, choose **No, do not export the private key** > **Next**.
3. In **Export File Format**, select **Base-64 encoded X.509 (.CER)** > **Next**.
4. In **File to Export**, specify a path and filename for the certificate > **Next**.
5. In **Completing the Certificate Export Wizard**, click **Finish**.

To export using Power Shell, run: ``S C:> $path = "C:\Temp\tenant4D.cer"

PS C:> $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2($path)

PS C:> $key = [Convert]::ToBase64String($cert.RawData)``

Export the private key

1. Right-click the certificate > **All Tasks** > **Export**.
2. In **Export Private Key**, choose **Yes, export the private key** > **Next**.If this option isn't available and you generated a self-signed certificate, ensure it included the -pe option.
3. In **Export File Format**, select **Personal Information Exchange - PKCS #12 (.PFX)**. Make sure **Include all certificates in the certification path if possible** is selected, and click **Next**.
4. In **File to Export**, specify a path and filename for the certificate > **Next**.
5. In **Completing the Certificate Export Wizard**, click **Finish**.

Create the tenant

Service Provider Foundation does not create user roles or define their scope (such as clouds), resources, or actions. Instead, the New-SCSPFTenantUserRole cmdlet creates an association for a tenant with a user role name. When that association is created, it also generates an ID that can be used for the corresponding ID for creating the role in System Center 2016 - Virtual Machine Manager.

You can also create user roles by using the Admin OData protocol service using the Developer's guide.

1. Run the SPF command shell as an Administrator.
2. Type following command to create the tenant. This command assumes that the `$key` variable contains the public key.

   ```
   PS C:\> $tenant = New-SCSPFTenant -Name "contoso.cloudspace.com" -IssuerName "contoso.cloudspace.com" -
   Key $key
   ```

3. Run this command to verify that the public key for the tenant was imported successfully:

   ```
   PS C:\> Get-SCSPFTrustedIssuer
   ```

   The next procedure uses the `$tenant` variable that you just created.

Create a tenant administrator role in VMM

1. Enter the following command and agree to this elevation for the Windows PowerShell command shell:

   ```
   PS C:\> Set-Executionpolicy remotesigned
   ```

2. Enter the following command to import the VMM module:

   ```
   PS C:\> Import-Module virtualmachinemanager
   ```

3. Use the Windows PowerShell T:Microsoft.SystemCenter.VirtualMachineManager.Cmdlets.New-SCUserRole cmdlet to create the user role. This command assumes the `$tenant` variable that was created as described in the procedure above.

   ```
   PS C:\> $TARole = New-SCUserRole -Name contoso.cloudspace.com -ID $tenant.Id -UserRoleProfile
   TenantAdmin
   ```

   Caution

   Note that if the user role was previously created by using the VMM Administration Console, its permissions would be overwritten by those specified by the **New-SCSUserRole** cmdlet.

4. Verify that the user role was created by verifying that it is listed in the **User Roles** in **Settings** workspace in the VMM Administration Console.
5. Define the following for the role by selecting the role and clicking **Properties** on the toolbar:

   - On the **Scope** tab, select one or more clouds.
   - On the **Resources** tab, add any resources such as templates.
   - On the **Actions** tab, select one or more actions.

   Repeat this procedure for every server assigned to the tenant.

The next procedure uses the `$TARole` variable that you just created.

Create a tenant self-service user role in VMM

1. Enter the following command to create a self-service user in SPF for the tenant you created.

```
PS C:\> $TenantSSU = New-SCSPFTenantUserRole -Name ContosoCloudSpaceSSU -Tenant $tenant
```

2. Create the corresponding tenant user role in VMM by entering the following command:

```
PS C:\> $vmmSSU = New-SCUserRole -Name ContosoCloudSpaceVMMSSU -UserRoleProfile SelfServiceUser -
ParentUserRole $TARole -ID $TenantSSU.ID
```

3. Verify that the user role was created by verifying that it is listed in the **User Roles** in **Settings** workspace in the VMM Administration Console. Notice that the parent of the role is the tenant administrator.

Repeat this procedure as needed for each tenant.

Manage usage metering in SPF

1/30/2019 • 2 minutes to read

You can configure System Center - Service Provider Foundation (SPF) to aggregate usage statistics for queries by the SPF Usage web service.

Before you start

Here's what you need:

- Servers running SPF, VMM, and Operations Manager. If needed, all these components can all be on the same computer.
- The Windows Azure Pack for Windows Server and API to provision IaaS.
- The Operations Manager server should have an Operations Manager Data Warehouse (OMDW) database. VMM management packs should be installed.
- A server running SQL Server with the Operations Manager Data Warehouse (OMDW).
- You can have the database for the OMDW and the database for Service Provider Foundation on the same server. Connection settings are stored in the Service Provider Foundation database.
- A Usage application pool identity credential that must be specified as a logon account to the OMDW databases. This account must have the db_DataReader and OpsMgrReader user mappings on each OMDW database. This is the same account specified for the Service Provider Foundation database.
- One or more virtual machines hosted by Hyper V (or VMM), and System Center Operations Manager.

Set up metering

Before you set up metering, check these resources:

- Learn about the SPF cmdlets.
- Read a blog post about usage metering.

Then set up metering as follows:

1. Create an instance of a server (using the **New-SCSPFServer** cmdlet) with the *ServerType* as OMDW.
2. Use the **New-SCSPFSetting** cmdlet to create a setting on that server (the one created in the previous step), that has the connection string to OperationsManagerDW database on the OMDW server.
3. Verify that the Application Pool account under which SPF_Usage runs has the ability to query OMDW.
4. Verify to make sure that the Windows Azure Pack calling account is a member of the SPF_User local security group on the server that has SPFinstalled.
5. Run the **New-SCSPFSetting** command with the parameters described in the following table.

NEW-SCSPFSETTING PARAMETER	VALUE
Value	Required. Must be a database connection string.
SettingType	Required. Must be **DatabaseConnectionString**.

NEW-SCSPFSETTING PARAMETER	VALUE
Name	Optional. This setting is recommended. Specify a meaningful name for each setting.
Server	Associates the setting with the sever from which usage metering is to be obtained. Must be a server object obtained from the Get-SCSPFServer cmdlet.

For example:

```
PS C:\> $omdwserver = New-SCSPFServer -Name "omdw.contoso.com" -ServerType OMDW
PS C:\>$setting = New-SCSPFSetting -Name mysetting -SettingType DatabaseConnectionString -Value
"Server=myomdwserver\myomdwinstance;Database=OperationsManagerDW;Trusted_Connection=True;Connect
Timeout=300" -Server $omdwserver
```

Use the Get-SCSPFSetting cmdlet to make changes to a particular setting. For example, the following code associates the setting with a different server, that is stored in the `$newSvr` variable.

```
PS C:\>$myset = Get-SCSPFSetting -Name "mySetting"
PS C:\>$myset.Server = $newSvr
```

Modify connection timeouts

The recommended connection timeout is 300 seconds, or 5 minutes. This value is also dependent on the volume of virtual machine usage metrics, SQL server edition (Enterprise recommended), hardware capacity, among other environment settings. You can change the connection timeout value using the Get-SCSPFSetting cmdlet

Import gallery items in SPF

12/6/2018 • 2 minutes to read

Gallery items are VM roles that serve as standard and reusable artifacts. These items can be used by hosting service providers, to provide offerings to their tenants. In Windows Azure Pack, you can add a gallery item to a tenant subscription plan. Virtual machine roles represent a scalable tier of virtual machines that can be provisioned by a tenant using a single process. Examples of workloads that can be created by virtual machine roles could include a single virtual machine, an Active Directory Domain Controller, a SQL Server cluster, or Internet Information Services (IIS) web farm. Learn more about gallery resources.

In System Center - Service Provider Foundation (SPF), you can import gallery items into System Center - Virtual Machine Manager (VMM) from downloaded resource packages. The gallery items are tracked in the SPFDB database. Gallery items will then be immediately available for viewing in the management portal, by Windows Azure Pack administrators.

SPF provides the following cmdlets for the gallery:

- Get-SCSPFVMRoleGalleryItem
- Get-SCSPFVMRoleGalleryItemIcon
- Get-SCSPFVMRoleGalleryItemPackage
- Import-SCSpfVMRoleGalleryItem
- Remove-SCSPFVMRoleGalleryItem
- Set-SCSPFVMRoleGalleryItem

Obtain a gallery resource

You can use the SPF Admin web service or cmdlets to get a gallery package, item, or the icon for an item. Portal developers can create UI elements and functionality, to offer tenants a compelling experience in selecting gallery items.

The following example shows how to use PowerShell to import a gallery item from a package and use its contents, and then remove it.

```
PS C:\> # The first command gets the path to the resource package and stores it in the $Path variable.
PS C:\> # The second command gets a System.IO.FileStream object of the package.
PS C:\> # The third command imports the package.
PS C:\> $Path = "c:\packages\create.resdefpkg"
PS C:\> $FStream = New-Object IO.FileStream $Path, Open
PS C:\> Import-SCSPFVMRoleGalleryItem -Package $FStream
PS C:\>
PS C:\> # Get an item from the gallery by specifying its name and store it in the $galItem variable.
PS C:\> $galItem = Get-ScSpfVmRoleGalleryItem -Name 570569955cbfb62b374358b34467020750f65c
PS C:\>
PS C:\> # Get the icon object by specifying the required parameters with the variable.
PS C:\> # The IconFileName parameter is explicitly specified in case the variable has a null value for the icon
file name.
PS C:\> $galItemIcon = Get-SCSPFVMRoleGalleryItemIcon -Name $galItem.Name -Publisher $galItem.Publisher -
Version $galItem.Version -IconFilename "contoso.ico"
PS C:\>
PS C:\> # Get the package of the gallery and stores it in the $galPkg variable. This cmdlets returns an
System.IO.MemoryStream object.
PS C:\> $galPkg = Get-SCSPFVMRoleGalleryItemPackage -Name 570569955cbfb62b374358b34467020750f65c -Publisher
Microsoft -Version 1.0.0.0
PS C:\>
PS C:\> # One use of the memory stream of the package is to save it to a file on your computer.
PS C:\> $fs = New-Object IO.Filestream "c:\@tmp\gal.bin", Create
PS C:\> $binwriter = New-Object IO.BinaryWriter $fs
PS C:\> $binwriter.Write($galPkg.ContentStream.ToArray())
PS C:\> $fs.Close()
PS C:\> $binwriter.Close()
PS C:\>
PS C:\> # Import the package that was just saved, using the PackageFilePath parameter.
PS C:\> Import-ScSpfVmRoleGalleryItem -PackageFilePath "C:\@tmp\gal.bin"
```

Automate and invoke runbooks from SPF

12/6/2018 • 2 minutes to read

You can use System Center Service Provider Foundation (SPF) and Service Management Automation (SMA) together to provide automated solutions for your tenants. You can configure events in SPF that the SMA web service will use.

Automate runbooks

You can automate runbooks using SMA, provided that you have configured SMA to use SPF,using the Set-SCSPFEventRegisration and Get-SCSPFEventRegistation cmdlets. This is shown in the following example:

```
PS C:\> # This command sets a runbook to be invoked when the Create event for a new virtual machine is raised.
PS C:\> Set-SCSPFEventRegistration -ResourceName "VMM.VirtualMachine" - ActionName "Create" -RunbookName
"Invoke-SampleCmdlet"
PS C:\>
PS C:\> # This command gets an event with the Action parameter and stores it in the $event_backup variable.
PS C:\> $event_backup = Get-SCSPFEventRegistration -Action "Backup"
```

Invoke runbooks

You can set a runbook in System Center - Orchestrator, to run whenever a new VM or service is created by remote calls to SPF with System Center Virtual Machine Manager (VMM).

- You can set the runbook to be invoked using the Windows PowerShell T:Microsoft.SystemCenter.Foundation.Cmdlet.Set-SCSPFExtensibleEventHandler cmdlet.
- SPF raises internal events to invoke the runbook. The runbook is continuously invoked, as long as the extensible event handler is enabled.
- SPF won't invoke the runbook if the VM or service was created by other means. For example, using Windows PowerShell cmdlets, or by using the VMM console.
- To support the infrastructure for invoking a runbook, SPF calls the **Start-SCOrchestratorRunbook** cmdlet internally. It doesn't need to be explicitly called by the user.
- Ensure you have applied the following before you call the T:Microsoft.SystemCenter.Foundation.Cmdlet.Set-SCSPFExtensibleEventHandler cmdlet:
  - The URL of the Orchestrator web service.
  - The identity settings for the SPF application pools in **Internet Information Services (IIS) Manager** must be included in the Orchestrator Users Group.

Then, invoke a runbook as follows:

1. Call the T:Microsoft.SystemCenter.Foundation.Cmdlet.Set-SCSPFExtensibleEventHandler with following parameters:

PARAMETER	VALUE
EventName	Specify either "VirtualMachineCreated" or "ServiceCreated".
OrchestratorUri	The URI to the Orchestrator web service.

PARAMETER	VALUE
RunbookPath	The local path to the runbook.
Enable	Specify to enable the runbook. To disable the runbook from being invoked, omit this parameter.

Example:

```
PS C:\> Set-SCSPFExtensibleEventHandler -EventName "VirtualMachineCreated" -OrchestratorUri
"http://east.contoso.com:82/Orchestrator2016/Orchestrator.svc" -RunbookPath "\SPF
Runbooks\Extensibility\VM Created" -Enable
```

2. To determine the setting for the extensible event handler, call the T:Microsoft.SystemCenter.Foundation.Cmdlet.Get-SCSPFExtensibleEventHandler cmdlet.

3. To disable a runbook from being invoked, repeat the T:Microsoft.SystemCenter.Foundation.Cmdlet.Get-SCSPFExtensibleEventHandler command, but without the **Enable*** parameter. You can also specify empty strings for the **OrchestratorUrl** and **Runbookpath** parameters, as shown in the following example:

```
PS C:\> Set-SCSPFExtensibleEventHandler -EventName "VirtualMachineCreated" -OrchestratorUri "" -
RunbookPath ""
```

Runbook parameters

This list of parameters is automatically provided to the runbook. A runbook doesn't need to process all the parameters it receives. It ignores parameters that have no purpose in the runbook.

Parameters for a new VM

The following table lists the parameters available when a new VM is created. All parameters are optional unless indicated.

PARAMETER	DATA TYPE
StampId (required)	Guid
Name (StampID name - required)	String
CloudId (required)	Guid
VMTemplateId	Guid
HardwareProfileId	Guid
VirtualHardDiskId	Guid
Description	String
CostCenter	String
Tag	String

PARAMETER	DATA TYPE
ComputerName	String
BlockDynamicOptimization	Boolean
CPULimitForMigration	Boolean
CPULimitFunctionality	Boolean
CPURelativeWeight	Int32
DelayStartSeconds	Int32
Domain	String
UserName	String
Password	String
DynamicMemoryBufferPercentage	Int32
DynamicMemoryEnabled	Boolean
DynamicMemoryMaximumMB	Int32
FullName	String
Memory	Int32
MemoryWeight	Int32
OrganizationName	String
StartAction	String
StartVM	Boolean
StopAction	String
CPUCount	Byte
Owner	PSObject
ProductKey	String
WorkGroup	String
TimeZone	Int32
RunAsAccountUserName	String

PARAMETER	DATA TYPE
LocalAdminRunAsAccountName	String
LocalAdminUserName	String
LocalAdminPassword	String
NewVirtualNetworkAdapterInput	PSObject
LinuxAdministratorSSHKey	String
LinuxDomainName	String

Parameters for a new service

The following table lists the parameters available when a new service is created. All parameters are optional unless indicated.

PARAMETER	DATA TYPE
StampID (required)	Guid
CloudID (required)	Guid
ServiceTempateId	Guid
NewServiceDeployment	PSObject
IgnorePlacementErrors	Boolean