

This document has been archived and will no longer be maintained or updated. For more information go to the [Storage Solutions Technical Documents page on Dell TechCenter](#) or contact support.

Dell Compellent Storage Center

Best Practices for Configuring the Dell Compellent SMI-S Provider for
Microsoft SCVMM 2012



Document Revisions

Date	Revision	Comments
04/11/2012	A	First Revision

THIS BEST PRACTICES GUIDE IS FOR INFORMATIONAL PURPOSES ONLY, AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

© 2012 Dell Inc. All rights reserved. Reproduction of this material in any manner whatsoever without the express written permission of Dell Inc. is strictly forbidden. For more information, contact Dell.

Dell, the *DELL* logo, the *DELL* badge, and Compellent are trademarks of Dell Inc. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

Contents

Document Revisions	2
Contents.....	3
General Syntax	6
Conventions	6
Preface	7
Audience	7
References	7
Purpose.	8
Introduction	9
Dell Compellent Storage Center Overview	9
Dell Compellent SMI-S Provider	9
Microsoft SCVMM 2012	9
Prerequisite Steps	10
Enable the Dell Compellent SMI-S Server.....	13
Configure Dell Compellent SMI-S User Settings.....	14
Overview	14
Create Enterprise Manager Client User	16
Run PowerShell Script to Create the SMI-S User and the Local Windows User.....	18
Configure SCVMM 2012 to Use Dell Compellent SMI-S	23
Add a Storage Device to SCVMM 2012	23
Create SCVMM 2012 Run As Account.....	25
Discover and Import Storage Device Information and Assign Classification	27
Adding Additional Dell Compellent Storage Centers to SCVMM 2012	35
Conclusion	40
Appendix A: Manual creation of Local User Account on the Data Collector Server	41

Tables

Table 1.	Document syntax.....	6
Table 2.	Prerequisite steps.....	10
Table 3.	User name password requirements	15

Figures

Figure 1:	Enable the Dell Compellent SMI-S Server	13
Figure 2:	Stop and restart the Data Collector service.....	13
Figure 3:	SMI-S user configuration	14
Figure 4:	Create an Enterprise Manager user	16
Figure 5:	Add a Storage Center for the SMIS Enterprise Manager user	16
Figure 6:	Storage Centers added to the Enterprise Manager client.....	17
Figure 7:	Verify that the Enterprise Manager user has been created	17
Figure 8:	Launch the SMIS User Configuration Script	18
Figure 9:	Trusted script prompt.....	19
Figure 10:	.Net warning message.....	19
Figure 11:	PowerShell Script Main Menu	19
Figure 12:	Create user accounts with PowerShell SMI-S Configuration Script	20
Figure 13:	Verify SMI-S Server configuration settings.....	21
Figure 14:	Add SSL certificate and associate it with the SMI-S user	22
Figure 15:	SCVMM 2012 Administrator console.....	23
Figure 16:	Add storage devices to SCVMM 2012.....	24
Figure 17:	Specify the storage devices discovery scope.....	24
Figure 18:	Create Run As account for SCVMM 2012	25
Figure 19:	Provide details for the SCVMM 2012 Run As account	25
Figure 20:	Select the new SCVMM 2012 Run As account.....	26
Figure 21:	Server information and account information for SCVMM 2012	27
Figure 22:	SCVMM 2012 Discover and import storage device information progress bar.....	27
Figure 23:	Import the SSL certificate into SCVMM 2012	28
Figure 24:	Issue with Microsoft KB2585542 may cause authentication failure	28
Figure 25:	Dell Compellent array shows as imported storage device	29
Figure 26:	Create new storage classification.....	30
Figure 27:	Assign a classification to the disk pool.....	31
Figure 28:	Confirm settings on the Summary screen.....	31
Figure 29:	SCVMM 2012 Jobs status window	32
Figure 30:	Successful completion of Sets Storage Array job.....	33
Figure 31:	Storage pool assigned to a Classification	34
Figure 32:	Additional Storage Center added to the Enterprise Manager client	35
Figure 33:	Discover an additional Storage Center by refreshing the Provider object.....	35
Figure 34:	Monitor the Jobs screen until Reads Storage Provider Job finishes.....	36
Figure 35:	Additional Storage Center Array added to SCVMM 2012	36
Figure 36:	Storage Properties General page.....	37

Figure 37:	Create and assign a Classification to additional storage pool	37
Figure 38:	Sets Storage Array Job	38
Figure 39:	Classifications and Pools.....	38
Figure 40:	Volumes listed under an assigned storage pool.....	39
Figure 41:	Rename managed Storage Pools.....	39
Figure 42:	Create a local user account on the Data Collector server	41
Figure 43:	Add the local user to the local administrators group.....	42
Figure 44:	Grant local user the “Log on as a service” right	43

General Syntax

Table 1. Document syntax

Item	Convention
Menu items, dialog box titles, field names, keys	Bold
Mouse click required	Click:
User Input	Monospace Font
User typing required	Type:
Website addresses	http://www.compellent.com
Email addresses	info@compellent.com

Conventions



Note

Notes are used to convey special information or instructions.



Timesaver

Timesavers are tips specifically designed to save time or reduce the number of steps.



Caution

Caution indicates the potential for risk including system or data damage.



Warning

Warning indicates that failure to follow directions could result in bodily harm.

Preface

Audience

This document is highly technical and intended for storage and server administrators, as well as other information technology professionals interested in learning more about how to configure the Dell Compellent SMI-S Provider version 1.4 for Microsoft SCVMM 2012.

This document assumes the reader has read, has formal training, or has advanced working knowledge of the following:

- Configuration and operation of the Dell Compellent Storage Center
- Configuration and operation of the Dell Compellent Enterprise Manager Client and Data Collector Server
- Configuration and operation of Microsoft SCVMM 2012

References

Reviewing the following documentation is highly recommended prior to referencing this best practices guide:

- Microsoft System Center Technical Documentation Library
<http://technet.microsoft.com/en-us/library/cc507089.aspx>
- Microsoft SCVMM 2012 Technical Documentation Library
<http://technet.microsoft.com/en-us/library/gg610610.aspx>
- Dell Compellent Documentation:
 - Enterprise Manager Installation and Users Guides
 - Storage Center Users Guide<http://knowledgecenter.compellent.com>

Purpose

The purpose of this document is to provide best practices for how to configure Microsoft System Center Virtual Machine Manager 2012 (SCVMM 2012) to work with the Dell Compellent SMI-S Provider version 1.4.



Please note that the information contained within this document provides general recommendations only and may not be applicable to all environments. Configurations may vary based upon individual circumstances, environments, or business needs.

Introduction

Dell Compellent Storage Center Overview

The Dell Compellent Storage Center is an enterprise class storage area network (SAN) that significantly lowers capital expenditures, reduces storage management and administration time, provides continuous data availability and enables storage virtualization. Storage Center's industry-standard hardware and sophisticated software manage data at the block-level, maximizing utilization, automating tiered storage, simplifying replication and speeding data recovery.

Dell Compellent SMI-S Provider

Storage Management Initiative Specification (SMI-S) is a standard interface specification developed by the Storage Networking Industry Association (SNIA). Based on the Common Information Model (CIM) and Web-Based Enterprise Management (WBEM) standards, SMI-S defines common protocols and data models that enable interoperability between storage vendor software and hardware.

The Dell Compellent SMI-S Provider version 1.4 works with the open source OpenPegasus CIM Server, which is included with the Enterprise Manager Data Collector. SMI-S can be configured during initial Data Collector installation or post-installation by modifying the Data Collector Manager properties. When SMI-S is enabled and configured, the Data Collector automatically installs and manages the Dell Compellent SMI-S Provider and the OpenPegasus CIM Server; no additional installation is required.

For more information about Dell Compellent SMI-S, please refer to the Dell Compellent Enterprise Manager Installation and Setup Guide.

Microsoft SCVMM 2012

Microsoft System Center 2012 is a cloud and datacenter management solution that provides a common management toolset for public and private cloud services and applications.

Virtual Machine Manager 2012 (as a component of the Microsoft System Center 2012 cloud and datacenter management suite) allows administrators to:

- Deliver Infrastructure as a Service (IaaS). Datacenter resources such as processing, networking, and storage can be pooled and virtualized and made available via self-service role-based user access.
- Apply cloud principles to provisioning and servicing datacenter applications with techniques like service modeling, service configuration and image based management.
- Server application virtualization allows applications and services to be managed independently from the underlying infrastructure.
- Optimize and manage multi-hypervisor environments such as Hyper-V, Xen and VMware.
- Dynamic optimization of datacenter resources based on workload demands.

Prerequisite Steps

This best practices guide assumes that the following steps have been completed. Complete the steps below before proceeding with this guide. Please refer to the documentation listed in **References** as required to complete the below steps.

Table 2. Prerequisite steps

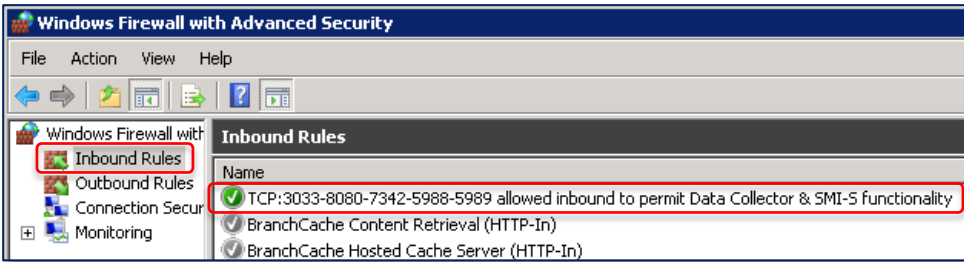
Step	<input checked="" type="checkbox"/>	Details
1	<input type="checkbox"/>	Verify that the Dell Compellent Enterprise Manager (EM) Data Collector version 5.5.5 has been installed on a server. This server will be referred to as the “Data Collector” server. The Data Collector server and the SCVMM 2012 server must be installed on separate physical or virtual servers that are members of the same Active Directory domain.
2	<input type="checkbox"/>	<p>If the Windows firewall is enabled on the Data Collector server, then create firewall exceptions to allow the following TCP ports inbound. In the example, a single Inbound Rule was created to allow these 5 TCP ports :</p> <ul style="list-style-type: none"> • TCP:3033 inbound (allows the Enterprise Manager Client Install to run from a different server) • TCP:8080 inbound (web service port) • TCP:7342 inbound (allows the Enterprise Manager Client (if installed on a different server) to communicate with the Data Collector Server) • TCP:5988 inbound (allows SCVMM 2012 to communicate with SMI-S on the Data Collector server via http) • TCP:5989 inbound (allows SCVMM 2012 to communicate with SMI-S on the Data Collector server via https)  <p>The screenshot shows the Windows Firewall with Advanced Security console. The left pane shows 'Inbound Rules' selected. The right pane shows a list of inbound rules. A red box highlights the rule named 'TCP:3033-8080-7342-5988-5989 allowed inbound to permit Data Collector & SMI-S functionality', which has a green checkmark icon indicating it is enabled.</p>
3	<input type="checkbox"/>	Verify that an instance of version 5.5.5 of the Enterprise Manager Client has been installed. The Client can be installed on the Enterprise Manager Data Collector server or a different server by running the installer located at: <a href="https://<ip_of_data_collector_server>:3033">https://<ip_of_data_collector_server>:3033
4	<input type="checkbox"/>	Verify that PowerShell has been installed on the Data Collector server. PowerShell is installed by default on Windows Server 2008.

Table 2: Prerequisite steps (continued)

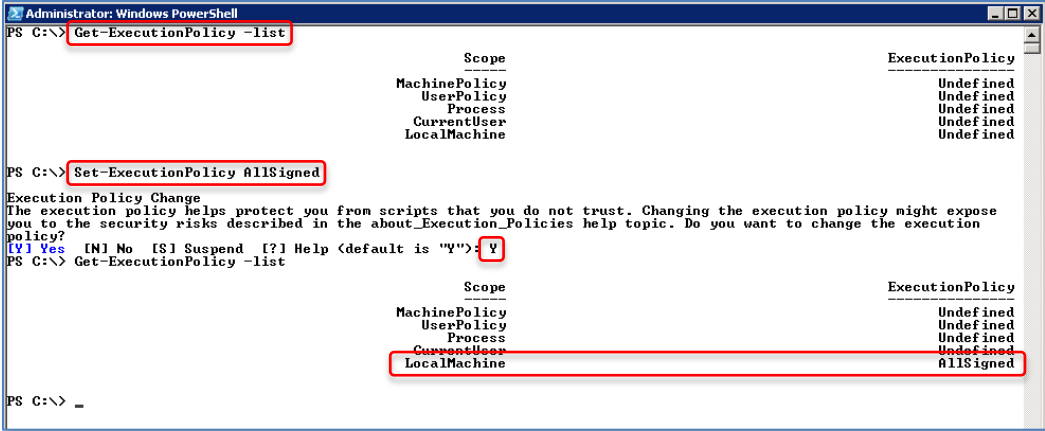
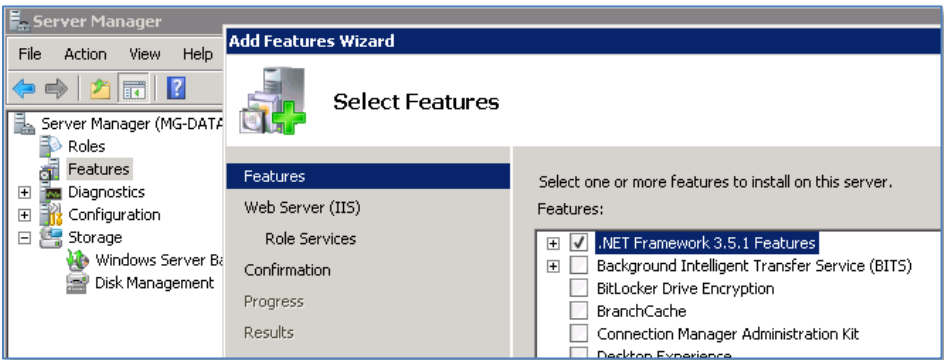
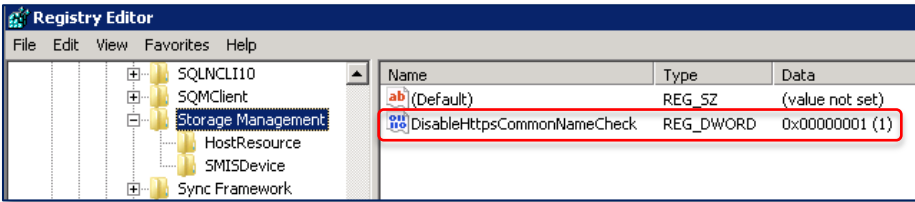
Step	<input checked="" type="checkbox"/>	Details
5	<input type="checkbox"/>	<p>Verify that the LocalMachine PowerShell ExecutionPolicy on the Data Collector server is set to something other than Undefined or Restricted. To verify the policy settings, open a PowerShell window and type the following command and press Enter.</p> <pre>Get-ExecutionPolicy -list</pre> <p>If the LocalMachine policy needs to be changed, use the following command where <policy> represents the ExecutionPolicy desired. In the example below, AllSigned is set as the LocalMachine Policy.</p> <pre>Set-ExecutionPolicy <policy></pre> 
6	<input type="checkbox"/>	<p>Verify that .NET 3.5 is installed on the Data Collector server. For example, on Server 2008, install from Start→Administrative Tools→Server Manager→Features.</p> 
7	<input type="checkbox"/>	<p>Verify that Microsoft SCVMM 2012 has been installed according to Microsoft best practices. The SCVMM 2012 server must be installed on a separate physical or virtual server than the Data Collector server, and both servers must be members of the same Active Directory domain.</p>

Table 2: Prerequisite steps (continued)

Step	<input checked="" type="checkbox"/>	Details
8	<input type="checkbox"/>	<p>The SCVMM 2012 Server does not accept the format of the Dell Compellent SSL certificate “CN” name when discovering storage with https (SSL) enabled. This causes the SCVMM 2012 discovery of the Dell Compellent storage via https (SSL) to fail.</p> <p>If communication between the SCVMM 2012 server and the Data Collector server will be configured to use SSL (https) (recommended), then disable CN name verification on the SCVMM 2012 server by adding a DWORD (32-bit) value to HKLM\Software\Microsoft\Storage Management per the documentation found at: http://technet.microsoft.com/en-us/library/gg610563.aspx</p> 

Once all the prerequisite steps are completed, then please proceed to the next section.

Enable the Dell Compellent SMI-S Server

Enable the SMI-S Server in the Enterprise Manager Data Collector GUI.

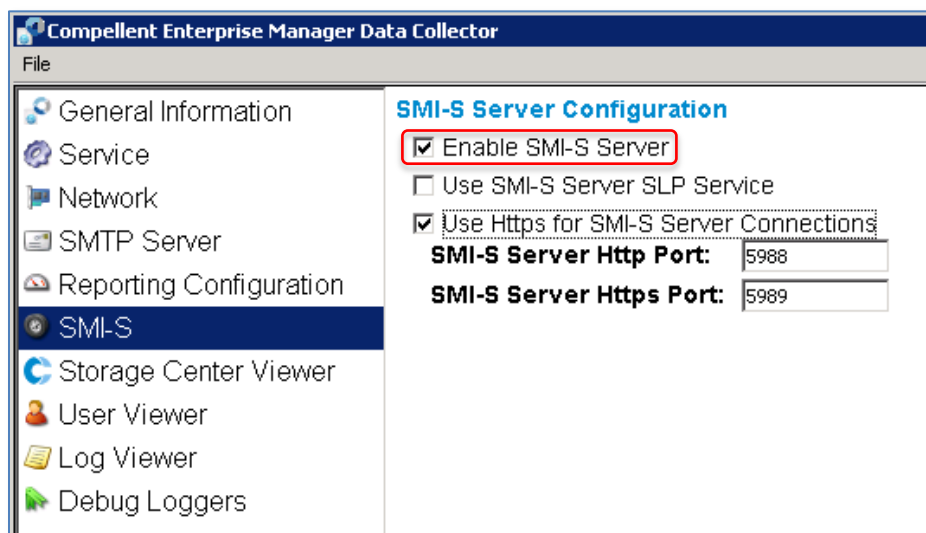


Figure 1: Enable the Dell Compellent SMI-S Server

- 1) On the Data Collector server, launch the Data Collector Manager GUI and complete the following steps, as shown in Figure 1:
 - Click on **SMI-S** in the left pane
 - Click on **Change** in the lower right corner of the Data Collector GUI screen
 - Check the box for **Enable SMI-S Server**
 - Leave the box for **Use SMI-S Server SLP Service** unchecked
 - Choose whether to use http or https for **SMI-S Server Connections**
 - To use https (recommended), check the box **Use Https for SMI-S Server Connections**
 - To use http, leave the box unchecked
 - If the ports 5988 and/or 5989 are changed from the defaults, then make any necessary adjustments to allow the ports through the Windows firewall (see **Table 2: Prerequisite Steps** for more information Windows firewall settings)

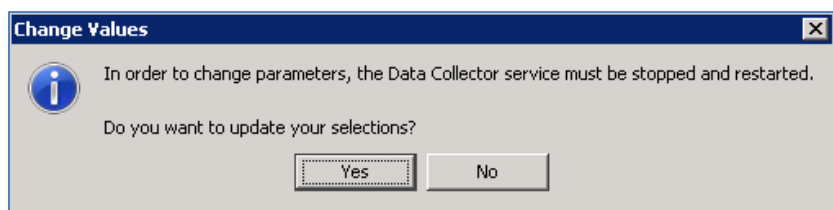


Figure 2: Stop and restart the Data Collector service

- 2) Click on **Apply Changes** in the lower right corner of the Data Collector GUI. When prompted, click **Yes** to restart the Data Collector service as shown in Figure 2.

Configure Dell Compellent SMI-S User Settings

Overview

Before SCVMM 2012 can access Dell Compellent Storage, a user account with the same name has to be configured in four places.



Note

In this document, a user named “SMIS” will be configured in the examples. Using the name “SMIS” is not required but is recommended for ease of management.

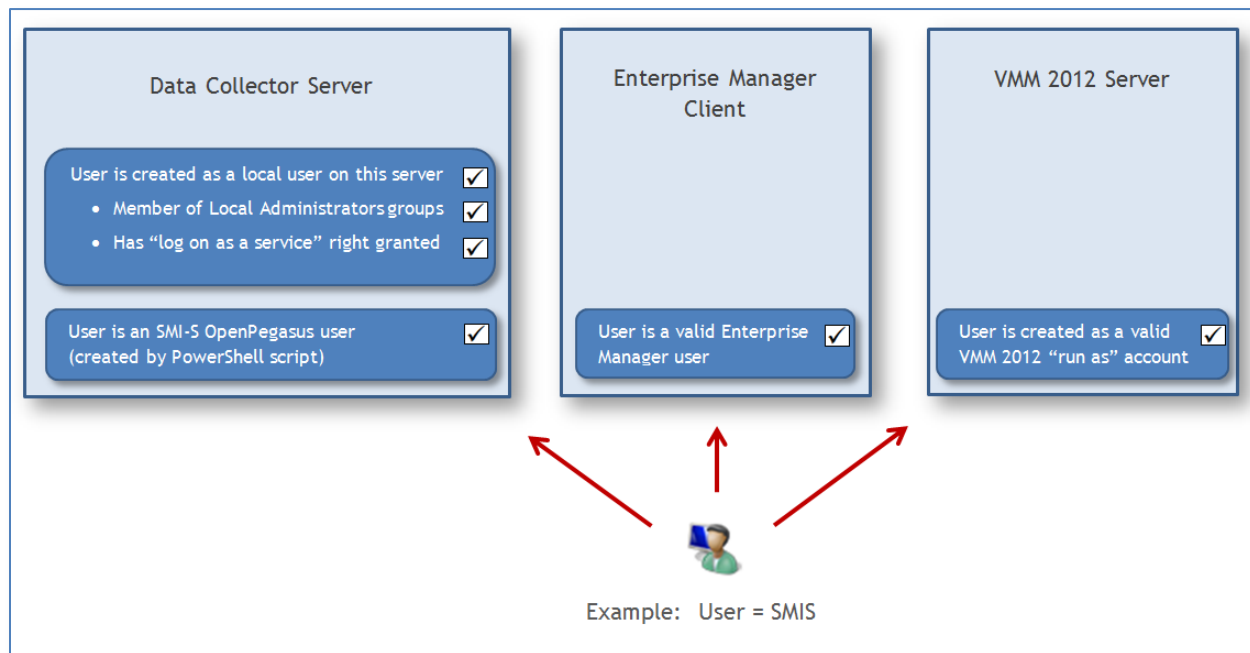


Figure 3: SMI-S user configuration

As shown in Figure 3, these four user instances are:

- Local Windows user account on the Data Collector server (that is a member of the local administrators group and is granted the "log on as a service" right)
- OpenPegasus SMI-S user
- Enterprise Manager Client user
- "run as" account on the SCVMM 2012 server (created using the SCVMM 2012 administrator console)

Table 3. User name password requirements

User Name	Instance	Password length restriction?	Passwords must match other instances of the SMIS user?
SMIS	Local User account on the Data Collector server	No (determined by the server's local password policy)	No
SMIS	Enterprise Manager Client user	Yes (8 characters or less)	Yes (these three SMIS user instances must all have matching passwords)
SMIS	OpenPegasus SMI-S user		
SMIS	"run as" account on the SCVMM 2012 server		

As shown in Table 3 above, there are some password requirements for the four instances of the SMIS user account.

- The user name must be the same for all four instances of the SMIS user
- The passwords must match for three of the four instances of the SMIS user as shown in Table 3
- It is possible for all four passwords to be set the same, however the password chosen must be eight characters or less and be able to satisfy the minimum password complexity requirements per the local password policy on the Data Collector server
 - For example, if the local password policy on the Data Collector server requires a minimum of 9 characters, then that instance of the SMIS user would have to use a different password than the password used for the other three instances

Below are the step-by-step instructions to create and configure these four user instances.

Create Enterprise Manager Client User

The figure consists of two side-by-side screenshots of the Enterprise Manager web interface. The left screenshot shows the 'Create New User' form, which includes fields for 'User' (SMIS), 'Password' (*****), 'Confirm Password' (*****), and 'Data Collector' (MG-DataC01). There are checkboxes for 'Create New User' and 'Create New Connection'. The right screenshot shows the 'Create New Connection' form, which includes fields for 'Name' (MG-DataC01), 'Host/IP' (172.16.23.121), and 'Port' (7342). Both forms have a 'LOGIN' button at the bottom right.

Figure 4: Create an Enterprise Manager user

- 1) Create a new Enterprise Manager User by using the logon screen of the Enterprise Manager Client (if using open security, as in Figure 4) or the Data Collector Manager GUI (if using enhanced security).



Note

The password chosen for this Enterprise Manager user must be 8 characters or less (please refer to Table 3). Record this password in a safe place and keep it handy as it will be needed in future steps below.

- 2) Choose the desired Data Collector Server from the drop-down list. If the desired Data Collector server is not listed, then create a new connection to the Data Collector server as shown in Figure 4 by entering the server name and the IP address. The Port field should be pre-populated with 7342 (which is the default port).

The figure shows a screenshot of the 'MG-DataC01: Compellent Enterprise Manager' web interface. The 'Storage Centers' section is highlighted with a blue bar. A red box highlights the 'Add Storage Center' button. Below this, there is a table with the following data:

Serial Number	Name
697	SC 12
699	SC 13
864	SC 5

To the right of the table, there is a form with the following fields:

- Host Name*: SC5.techsol.local
- User Name: mglaser
- Password: *****

Figure 5: Add a Storage Center for the SMIS Enterprise Manager user

- 3) After logging in to Enterprise Manager with the new user SMIS, add one or more Dell Compellent Storage Centers that will be made available to SCVMM 2012, as shown in Figure 5.
 - Select from the available listing of Storage Centers, or
 - Choose **Add Storage Center** if the desired Storage Center is not listed, and provide the Host Name or IP address of the Storage Center, along with valid administrator user credentials to that storage center.

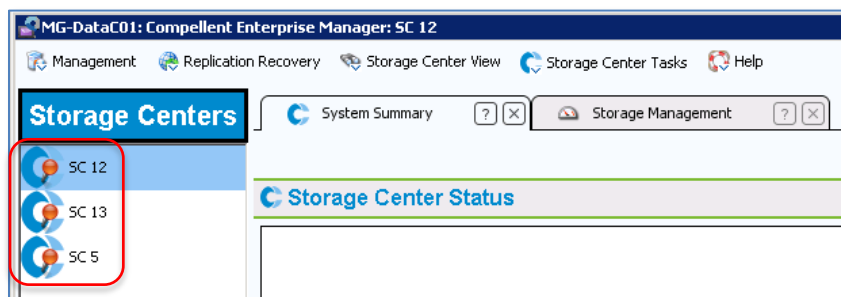


Figure 6: Storage Centers added to the Enterprise Manager client

- 4) Once one or more Storage Centers have been added, close out of the Enterprise Manager client. In this example, three Storage Centers have been added as shown in Figure 6.



Note

It is possible to add additional storage arrays later on if that becomes necessary. To do so, simply log in to the Enterprise Manager client as the SMIS user and add additional Storage Centers by repeating steps 2 and 3 above. They will then become available to SCVMM 2012 after refreshing the storage provider in SCVMM 2012.

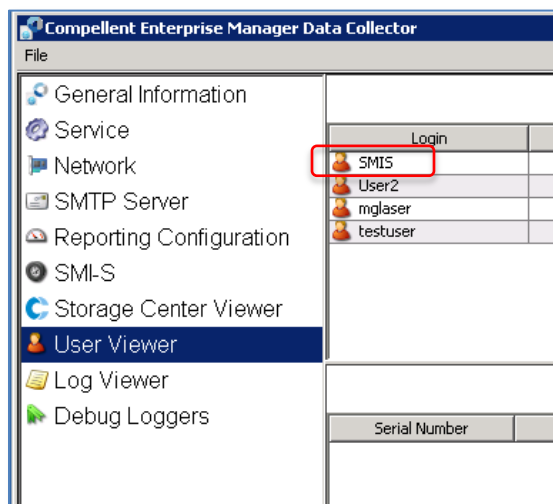


Figure 7: Verify that the Enterprise Manager user has been created

- 5) On the Data Collector server, under **User Viewer** in the Data Collector GUI, verify that the new user is listed as shown in Figure 7. If the user is not yet listed, click on the **Refresh** button.

Run PowerShell Script to Create the SMI-S User and the Local Windows User

The **Launch SMIS User Configuration Script** via PowerShell script does two things:

- Creates the Dell Compellent SMI-S OpenPegaus user
- Automates the process of creating a matching local Windows user account on the Data Collector server (if this user account does not already exist)

The recommendation is to allow the PowerShell script to create the local Windows user account on the Data Collector server. If manual creation of this Windows user is preferred, please follow the steps in **Appendix A** before running the PowerShell script below. When the PowerShell Script runs, it will verify the presence of the local Windows user account and skip the steps associated with the creation of that user. The example below assumes that the PowerShell Script will be used to create the local Windows user account.



Note

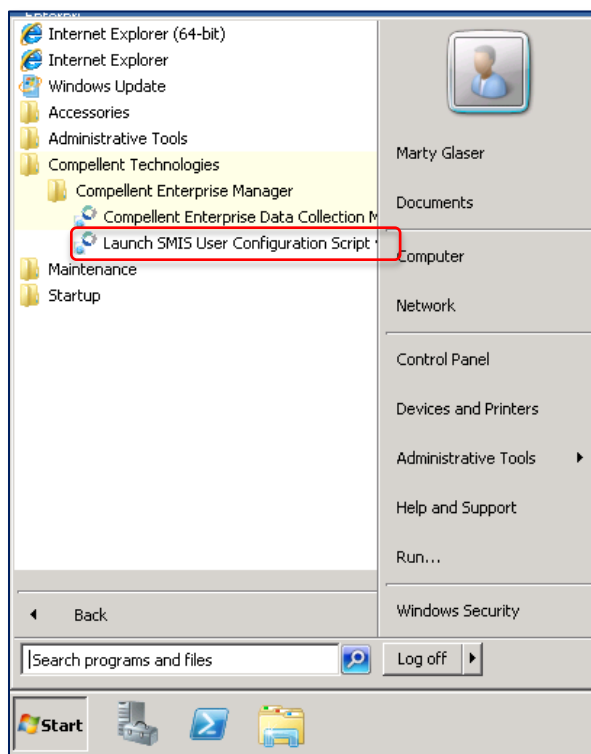


Figure 8: Launch the SMIS User Configuration Script

- 1) As shown in Figure 8, on the Data Collector server, go to **Start → All programs → Compellent Technologies → Compellent Enterprise Manager** and select **Launch SMIS User Configuration Script via PowerShell**.



Note

If the PowerShell Script fails to launch, verify that the PowerShell **LocalMachine Execution Policy** is set correctly. For more information on how to verify and set the LocalMachine Execution Policy, see **Table 2: Prerequisite Steps**.

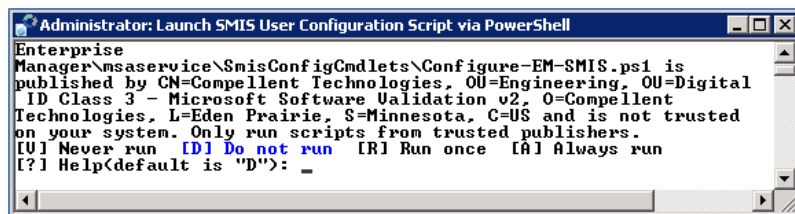


Figure 9: Trusted script prompt

- 2) Depending on the LocalMachine Execution Policy for PowerShell on the Data Collector server, a security prompt may appear as shown in Figure 9. Type R or A and press Enter to continue. For more information on PowerShell ExecutionPolicy settings, see [Table 2: Prerequisite steps](#).

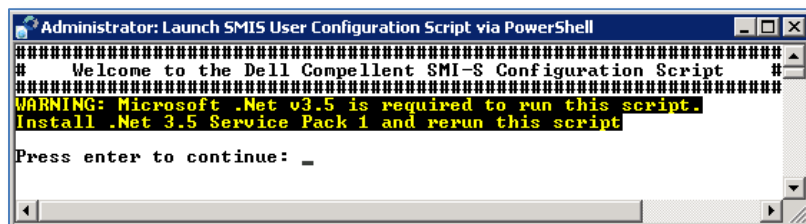


Figure 10: .Net warning message

- 3) If a .Net v3.5 warning message appears as shown in Figure 10, press Enter to exit the script. Install .Net 3.5, and then rerun the PowerShell Script starting at Step 1 in this section. For more information, see [Table 2: Prerequisite steps](#).

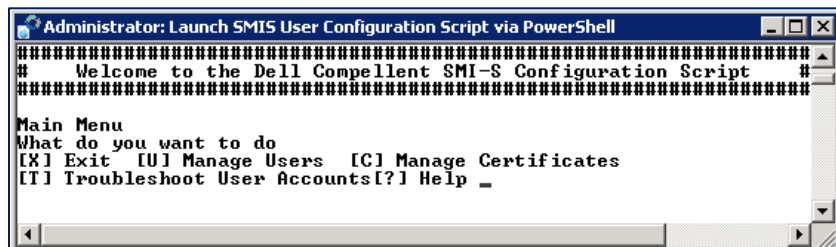


Figure 11: PowerShell Script Main Menu

- 4) The Script Main Menu will then be displayed as shown in Figure 11.

```

Administrator: Launch SMIS User Configuration Script via PowerShell
#####
# Welcome to the Dell Compellent SMI-S Configuration Script #
#####

Main Menu
What do you want to do
[X] Exit  [U] Manage Users  [C] Manage Certificates  [T] Troubleshoot User Accounts  [?] Help u

Manage Users
What do you want to do
[X] Exit to main menu  [L] List SMI-S Users  [A] Add SMI-S User  [R] Remove SMI-S User  [E] List EM Users
[U] List Local Admin Users[?] Help a

The user needs to have a matching Enterprise Manager user name with the same password as what you enter below.

Please choose an EM user
Choose an item
[X] Cancel and exit back to user menu  [1] 1 - mglasser  [2] 2 - SMIS  [?] Help 2
This will create an SMI-S user with the name [SMIS]. Please enter the EM user password:
Password: *****
Confirm Password: *****

A corresponding local Windows user [SMIS] does not exist
Do you want to create a new local windows admin user account?
[O] Ok  [C] Cancel  [?] Help o

Do you want to use the same password for the windows user? The SMI-S user and the Windows user do not need to have the
same password.
Use same password?
[Y] Yes  [N] No  [?] Help y

The user [SMIS] does not have logon-as-a-service rights
Press Ok to add the logon-as-a-service right.
[O] Ok  [C] Cancel  [?] Help o
True

Would you like to set the [Password Never Expires] flag for the user [SMIS]?
This is often used for service oriented accounts
[Y] Yes  [N] No  [?] Help y
User added successfully.

Manage Users
What do you want to do
[X] Exit to main menu  [L] List SMI-S Users  [A] Add SMI-S User  [R] Remove SMI-S User  [E] List EM Users
[U] List Local Admin Users[?] Help _

```

Figure 12: Create user accounts with PowerShell SMI-S Configuration Script

Referring to Figure 12, complete the steps 5 - 15 below:

- 5) At the Main Menu, type **U** to manage users and press **Enter**.
- 6) Under Manage Users, type **A** and press **Enter** to add an SMI-S User.
- 7) Select the number of the Enterprise Manager (EM) user, which in this example is **2** (for the user **SMIS**) and press **Enter**. This is the same user that was created on page 16.
- 8) Enter the EM user password (same password used on Page 16) and press **Enter**.



Note

This password must match the password that was used for the SMIS user created on page 16. See Table 3 for more information on password requirements.

- 9) Enter the password a second time to confirm it, and press **Enter**.
- 10) If a corresponding local Windows user does not exist, then enter **O** and press **Enter** to allow the script create this user.
- 11) Type **Y** to use the same password, or **N** to enter a different password. Using the same password is possible only if it meets the minimum complexity requirements for your Windows environment. For more information on password requirements, see Table 3.

- 12) To grant the local Windows user the logon-as-a-service right, type **O** and press **Enter**.
- 13) To set the password to never expire (recommended), type **Y** and press **Enter**.
- 14) To verify the creation of these user accounts, use the **List** menu options in the script (if desired).
- 15) When finished, Type **X** and press **Enter** to return to the PowerShell script main menu.

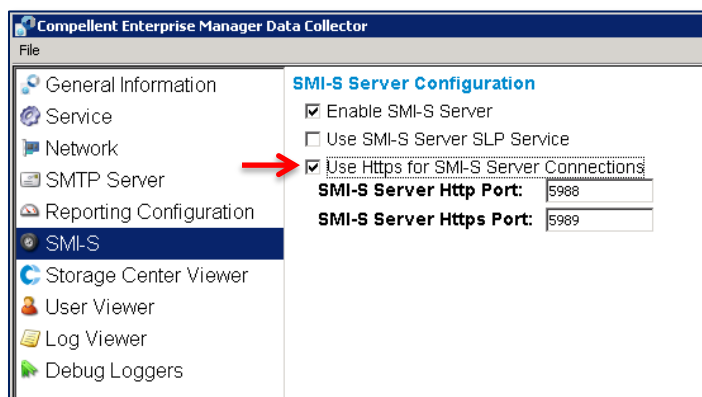


Figure 13: Verify SMI-S Server configuration settings

- 16) If SMI-S was configured to use Https, then an SSL certificate needs to be associated with the SMI-S user. To verify whether http or https was selected, view the SMI-S Server Configuration settings in the Data Collector GUI as shown in Figure 13.
 - a) If the option **Use Https for SMI-S Server Connections** is enabled as shown, then continue with Step 17 below to use the PowerShell Script to assign an SSL certificate to the SMIS user.
 - b) If the box is left unchecked, then http will be used and therefore assigning an SSL certificate is unnecessary. Type **X** and press **Enter** to close out of the PowerShell Script and go to the next section on page 23, **Configure SCVMM 2012 to Use Dell Compellent SMI-S**.

```

Administrator: Launch SMIS User Configuration Script via PowerShell
#####
# Welcome to the Dell Compellent SMI-S Configuration Script #
#####

Main Menu
What do you want to do
[X] Exit [U] Manage Users [C] Manage Certificates [T] Troubleshoot User Accounts [?] Help c

Manage Certificates
What do you want to do
[X] Exit to main menu [L] List certificates [A] Add default server SSL certificate to SMI-S trust store
[R] Remove a certificate[?] Help a

A user association is required because the default certificate is a self-signed certificate
Pick a user to associate the default certificate with:
[X] Cancel and exit back to menu [1] 1 - SMIS [?] Help 1
Certificate added successfully.

Manage Certificates
What do you want to do
[X] Exit to main menu [L] List certificates [A] Add default server SSL certificate to SMI-S trust store
[R] Remove a certificate[?] Help l
Certificates:

Issuer          : /C=US/ST=Minnesota/L=Eden Prairie/O=DELL/OU=Compellent/CN=MG-DataC02
Subject         : /C=US/ST=Minnesota/L=Eden Prairie/O=DELL/OU=Compellent/CN=MG-DataC02
SerialNumber    : 4294967295
RegisteredUserName : SMIS
CertificateType  : Self-signed identity
ValidNotBefore  : Feb 15, 2012 17:38:26 <+0000>
ValidNotAfter   : Feb 12, 2022 17:38:26 <+0000>
IssuerIntens    :
SubjectItem     :

Manage Certificates
What do you want to do
[X] Exit to main menu [L] List certificates [A] Add default server SSL certificate to SMI-S trust store
[R] Remove a certificate[?] Help x

Main Menu
What do you want to do
[X] Exit [U] Manage Users [C] Manage Certificates [T] Troubleshoot User Accounts [?] Help x

Press enter to continue: _

```

Figure 14: Add SSL certificate and associate it with the SMI-S user

- 17) To add an SSL certificate and associate it with the SMI-S user, refer to Figure 14 while completing steps 18 - 24 below.
- 18) From the PowerShell Script Main Menu, type C and press Enter to manage certificates.
- 19) From the Manage Certificates menu, type A and press Enter to add an SSL certificate to the SMI-S trust store.
- 20) When prompted to associate a user, select the desired SMI-S user (the user "SMIS" in this example). Type the number for that user and press Enter to select the user.
- 21) The PowerShell Script will return the result **Certificate Added Successfully** and then return to the Manage Certificates menu.
- 22) Type L and press Enter to verify the certificate details.
- 23) Type X and press Enter to return to the main menu.
- 24) Type X and press Enter twice to close out of the PowerShell command window.

Configure SCVMM 2012 to Use Dell Compellent SMI-S

Now that the SMI-S user settings along with the SMI-S Server configuration have been set up correctly on the Data Collector server, Microsoft SCVMM 2012 can now be configured to work with the Dell Compellent SMI-S Provider to manage Dell Compellent storage.



Note

The Data Collector server and the SCVMM 2012 server must be members of the same domain but reside on separate physical or virtual servers.

Add a Storage Device to SCVMM 2012

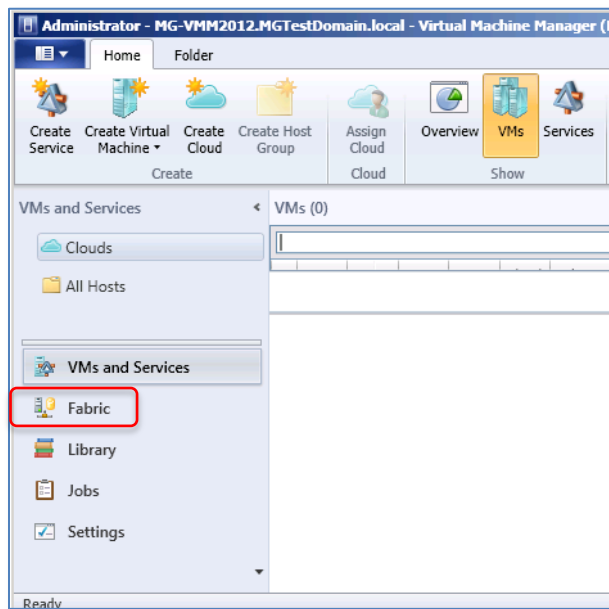


Figure 15: SCVMM 2012 Administrator console

- 1) On the server hosting Microsoft SCVMM 2012, start the SCVMM 2012 Administrator console. Under the **Home** tab, select the **Fabric** workspace as shown in Figure 15.

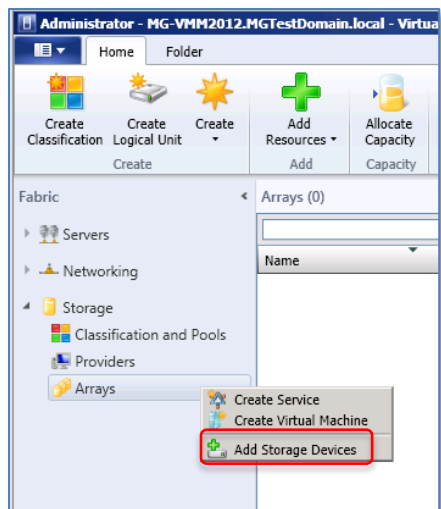


Figure 16: Add storage devices to SCVMM 2012

- 2) Expand **Storage**, right click on **Arrays** and choose **Add Storage Devices** from the drop down list as shown in Figure 16.

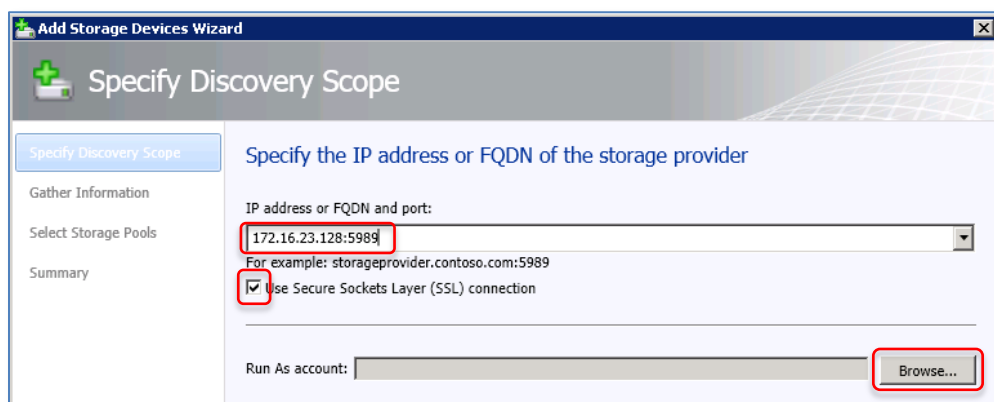


Figure 17: Specify the storage devices discovery scope

- 3) In the **Add Storage Devices Wizard** screen, enter the IP address or fully qualified domain name (FQDN) of the Data Collector server along with the correct port number.
 - For http, uncheck the box for **Use Secure Sockets Layer (SSL) connection** and specify the correct port (5988 is the default)
 - For https, check the box for **Use Secure Sockets Layer (SSL) connection** and specify the correct port (5989 is the default)



Note

If using https (SSL), a registry change needs to be made to the SCVMM 2012 server to disable CN name verification, otherwise the SLL certificate import will fail. To make the registry change, please insure that step 8 in Table 2 under **Prerequisite Steps** has been completed before continuing.

- 4) Click on the **Browse** button to the right of the **Run As** account field.

Create SCVMM 2012 Run As Account

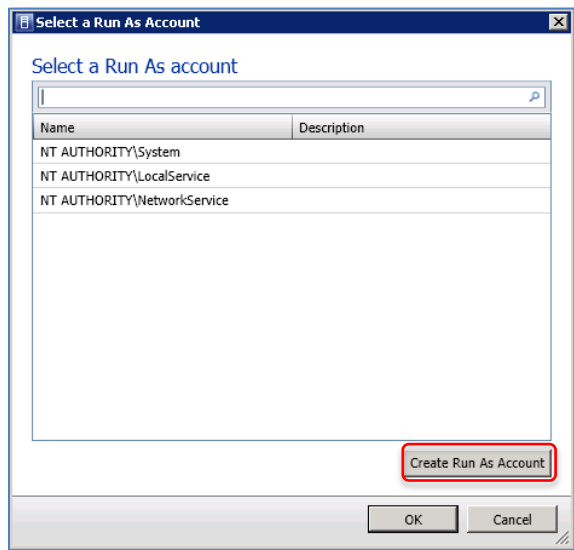


Figure 18: Create Run As account for SCVMM 2012

- 1) At the **Select a Run As Account** screen, click on the **Create Run As Account** button as shown in Figure 18.

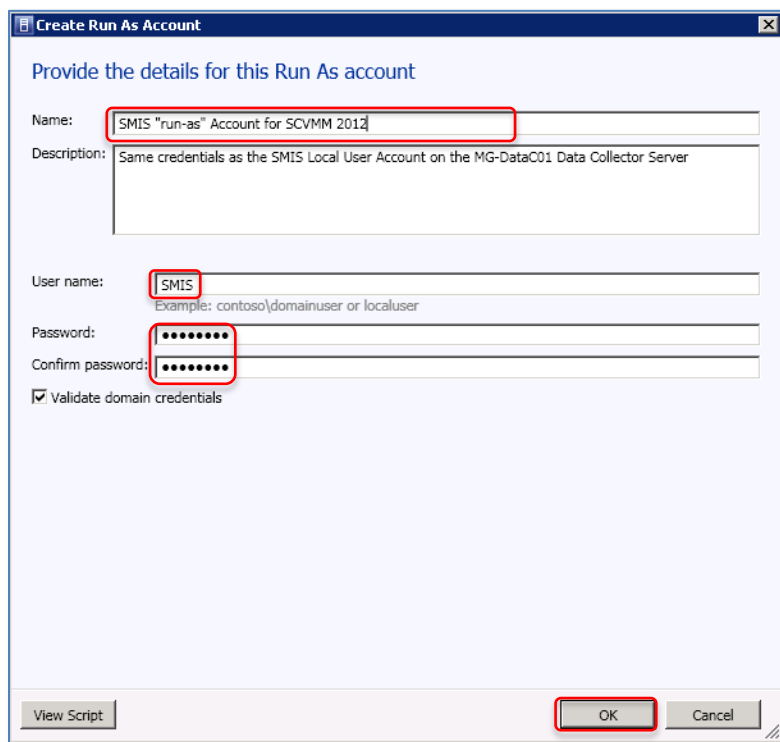


Figure 19: Provide details for the SCVMM 2012 Run As account

- 2) As shown in Figure 19, provide a descriptive name (and description if desired) for the Run As account.
- 3) Enter the user name and password.



Provide the same user name and password that were used to create the EM user (page 16) and the OpenPegasus SMI-S user and local Windows user (created using the PowerShell Script on page 20). See **Table 3** for more information on user and password requirements.

- 4) Click on the **OK** button to return to the previous screen.

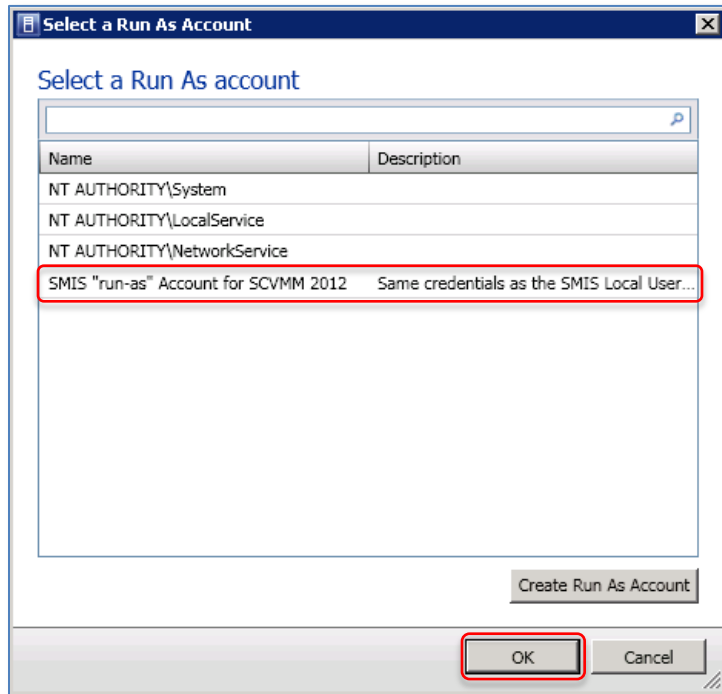


Figure 20: Select the new SCVMM 2012 Run As account

- 5) Click on the new **Run As Account** to highlight it, and then click on the **OK** button, as shown in Figure 20.

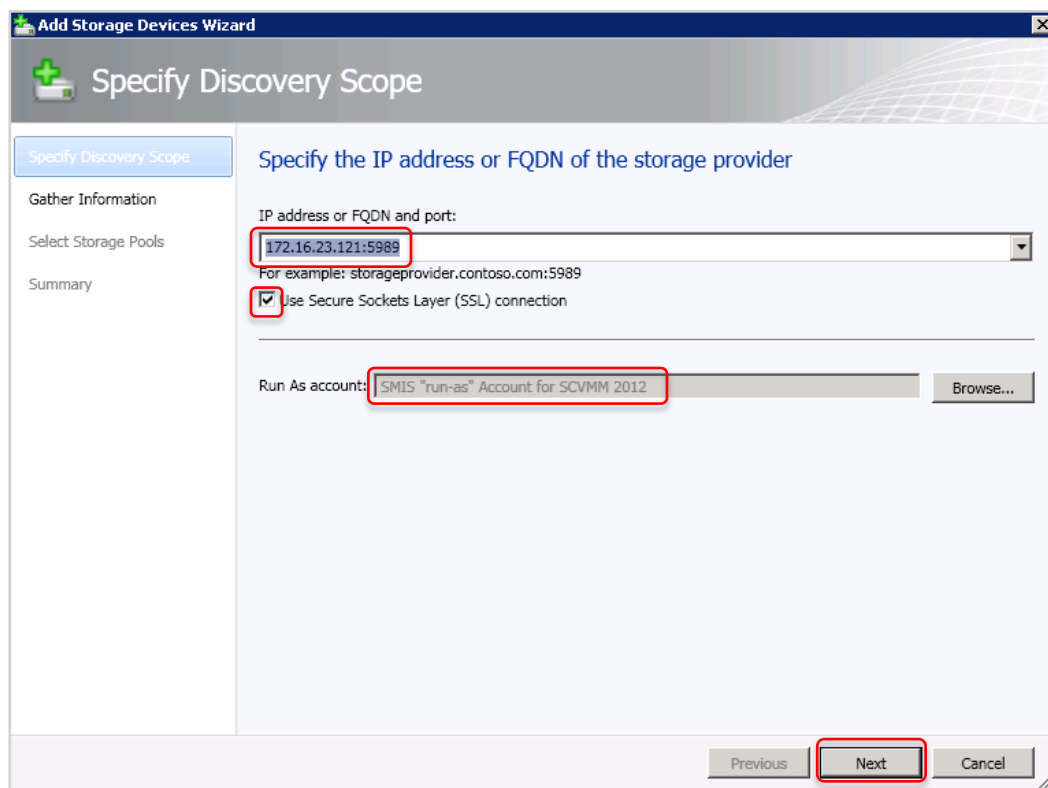


Figure 21: Server information and account information for SCVMM 2012

- 6) Verify that the new user is displayed in the **Run As account** field as shown in Figure 21. Also verify that the IP Address (or fully qualified domain name) followed by the port number is still listed correctly, and if https is desired, that the SSL box is checked. Then click on the **Next** button.

Discover and Import Storage Device Information and Assign Classification

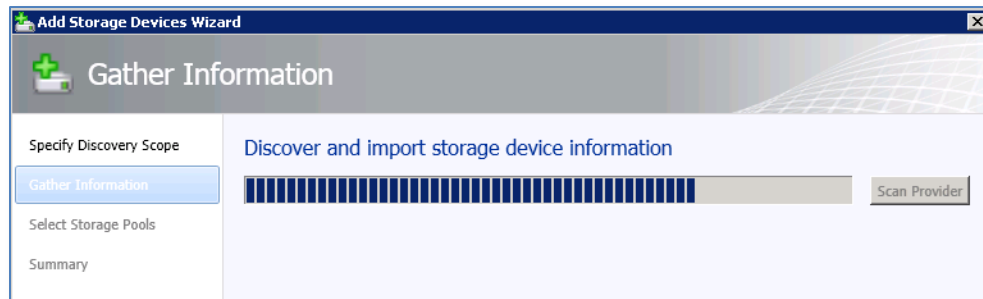


Figure 22: SCVMM 2012 Discover and import storage device information progress bar

- 1) As shown in Figure 22, SCVMM 2012 will display a progress bar as it begins to import the storage device information. The import process may require several minutes to complete.

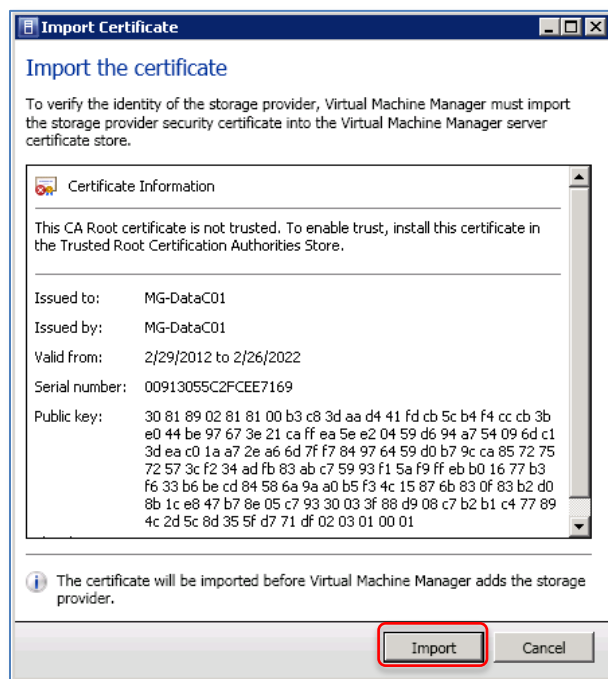


Figure 23: Import the SSL certificate into SCVMM 2012

- 2) If using https, SCVMM 2012 will need to import the SSL certificate. Click on the **Import** button as shown in Figure 23 when prompted. If using http, this prompt will not occur.

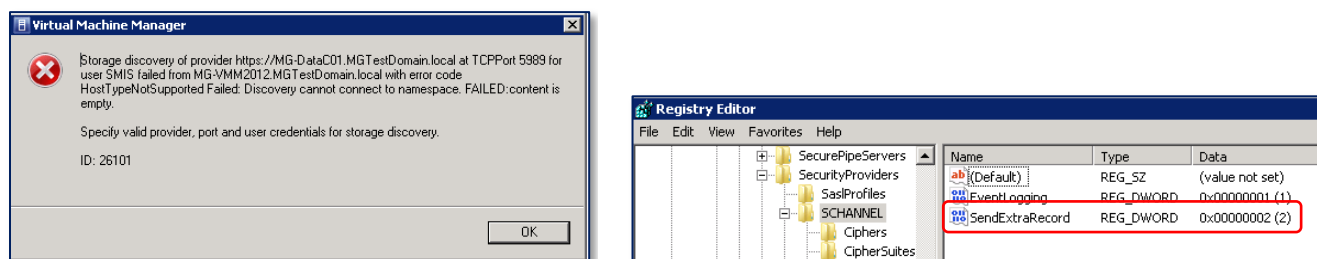


Figure 24: Issue with Microsoft KB2585542 may cause authentication failure



Note

If using https (SSL), it may be necessary to address an authentication failure (content is empty) caused by the January 2012 Microsoft Security Update KB2585542 for Server 2008 R2. If this error as shown in Figure 24 is experienced, follow the instructions at <http://support.microsoft.com/kb/2643584> to modify the system registry to add a new DWORD (32-bit) value to `HKLM\System\CurrentControlSet\Control\SecurityProviders\CHANNEL` as shown in Figure 24.

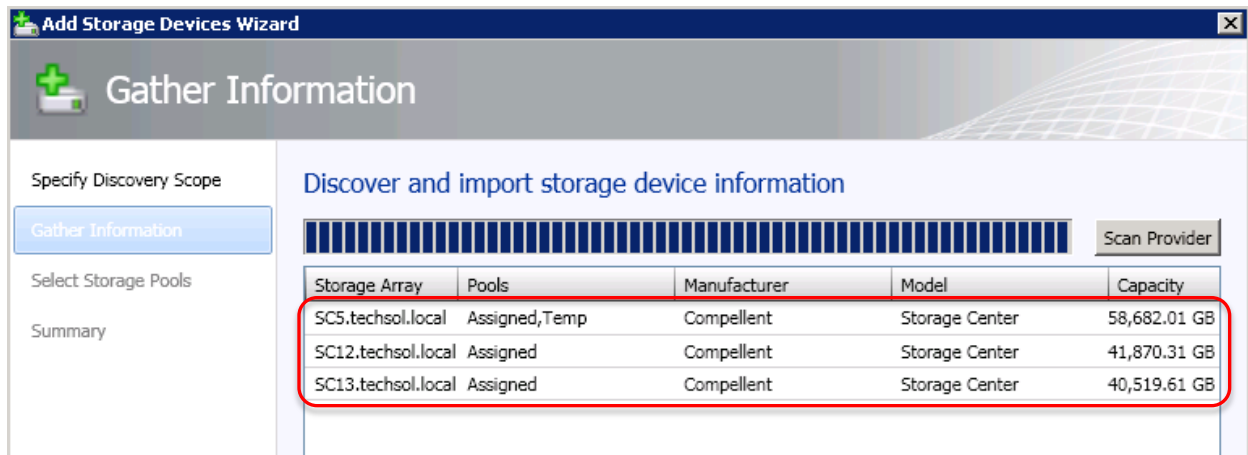


Figure 25: Dell Compellent array shows as imported storage device

- 3) Once the import process has finished, the Dell Compellent Storage Center will be displayed as shown in the example in Figure 25. In this example, three storage centers have been discovered and imported. Click on the **Next** button.

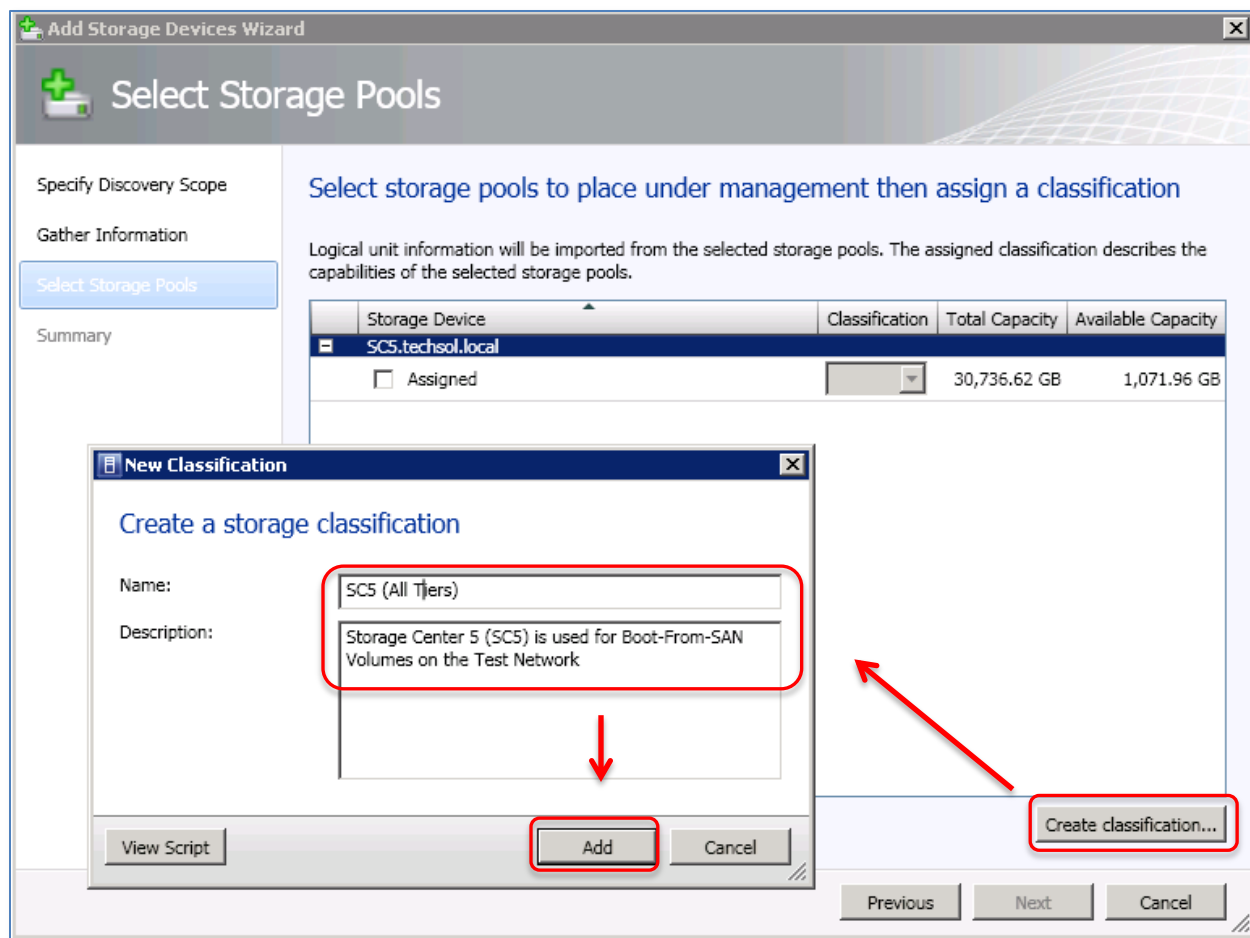


Figure 26: Create new storage classification

- 4) On the next screen, click on the **Create Classification** button to define one or more classifications for your imported Storage Centers. A “classification” is meant to describe the capabilities of the selected storage pool. Because Dell Compellent Storage Centers typically feature automated disk tiering within a single disk pool, the description might include a summary of the types of disk and tiers in the array, or other attributes, such as the array’s primary use or location, as shown in Figure 26.
- 5) Once a name and description have been provided for the storage classification, then click on the **Add** button as shown in Figure 26.
- 6) Repeat steps 4 and 5 to create additional storage classifications. In this example, three classifications were created: one for each of the three Storage Centers SC5, SC12 and SC13.

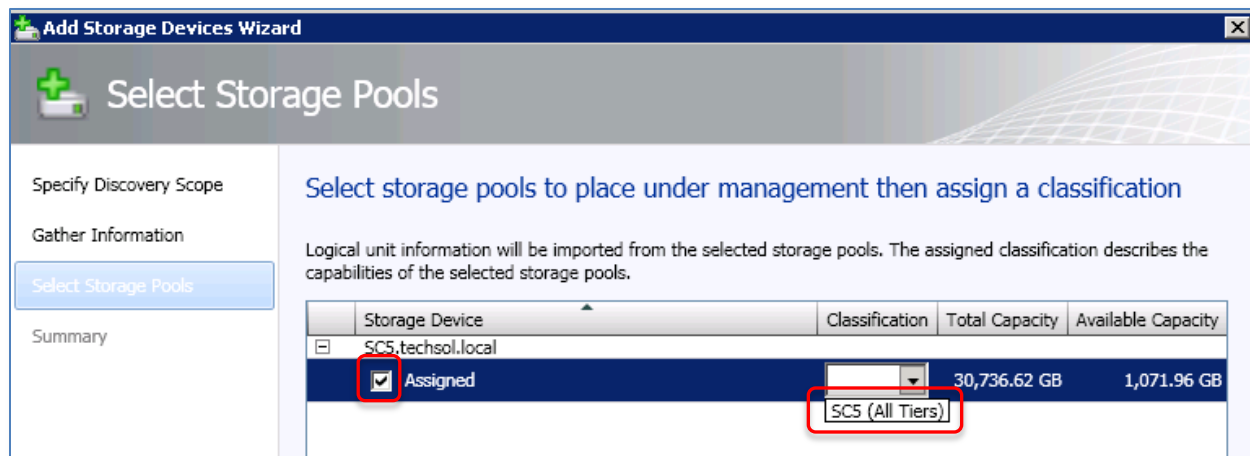


Figure 27: Assign a classification to the disk pool

- 7) Now that one or more classifications have been defined, check the box in front of **Assigned**, and then click on the drop down arrow under the Classification column and choose the desired storage classification as shown in Figure 27. Then click on the **Next** button.



Assign storage classifications to Storage Centers one at a time. Allow the job to finish, and then assign a classification to the next Storage Center. Assigning classifications to multiple Storage Centers at the same time may result in storage discovery failures with SCVMM 2012.

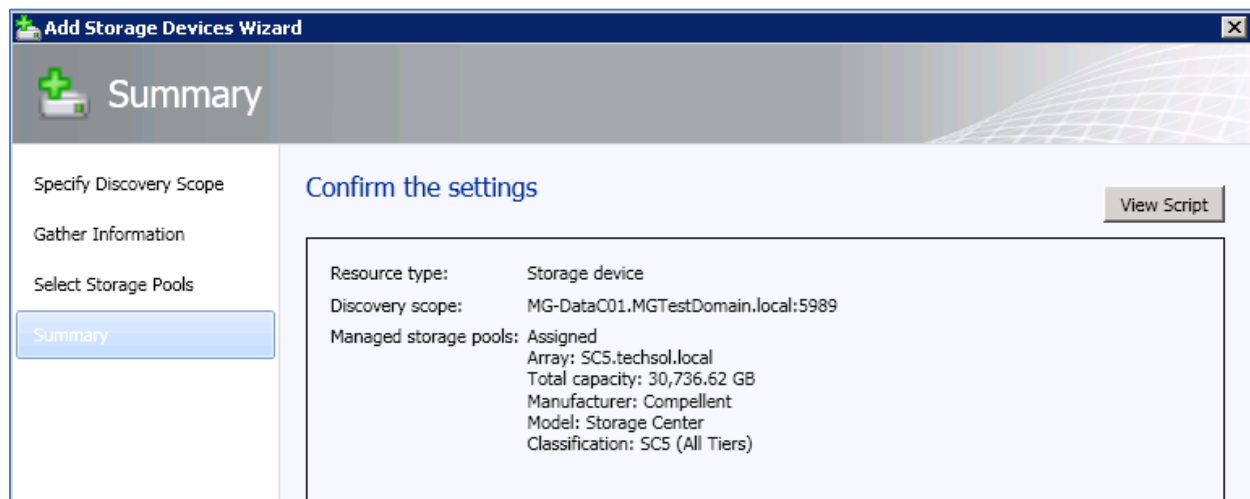


Figure 28: Confirm settings on the Summary screen

- 8) A summary screen will display the details for the managed storage pool. Click on **Finish** to complete the wizard.

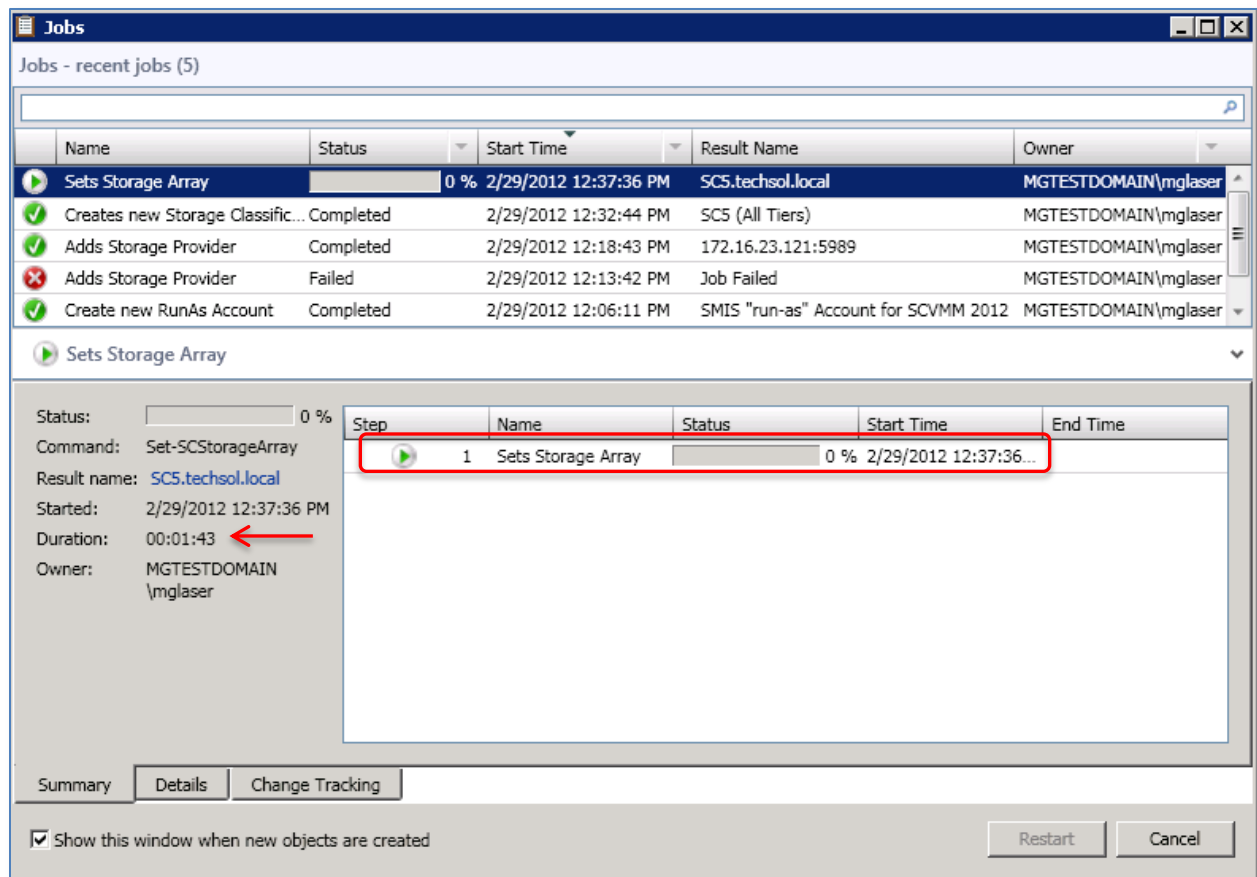


Figure 29: SCVMM 2012 Jobs status window

- 9) The Jobs status window will display the **Sets Storage Array** job with a progress bar under the Status column. If the Jobs window is not set to display automatically, then job history and status can be viewed by clicking on **Jobs** in the left navigation pane of the SCVMM 2012 Administrator console.
- 10) The Duration line as shown in Figure 29 will indicate the Job's run time. Refresh the screen to update the run time. Depending on the configuration of the Storage Center, the Job may require up to 30 minutes or more to complete.



Note

The Job progress bar in SCVMM 2012 will not show incremental progress as the Job runs, so it may appear as though the Job has stopped responding. It will stay at 0% and jump to 100% when it has finished. If a Storage Center has a large number of volumes, discovery will require extra time, up to 30 minutes or more per Storage Center.

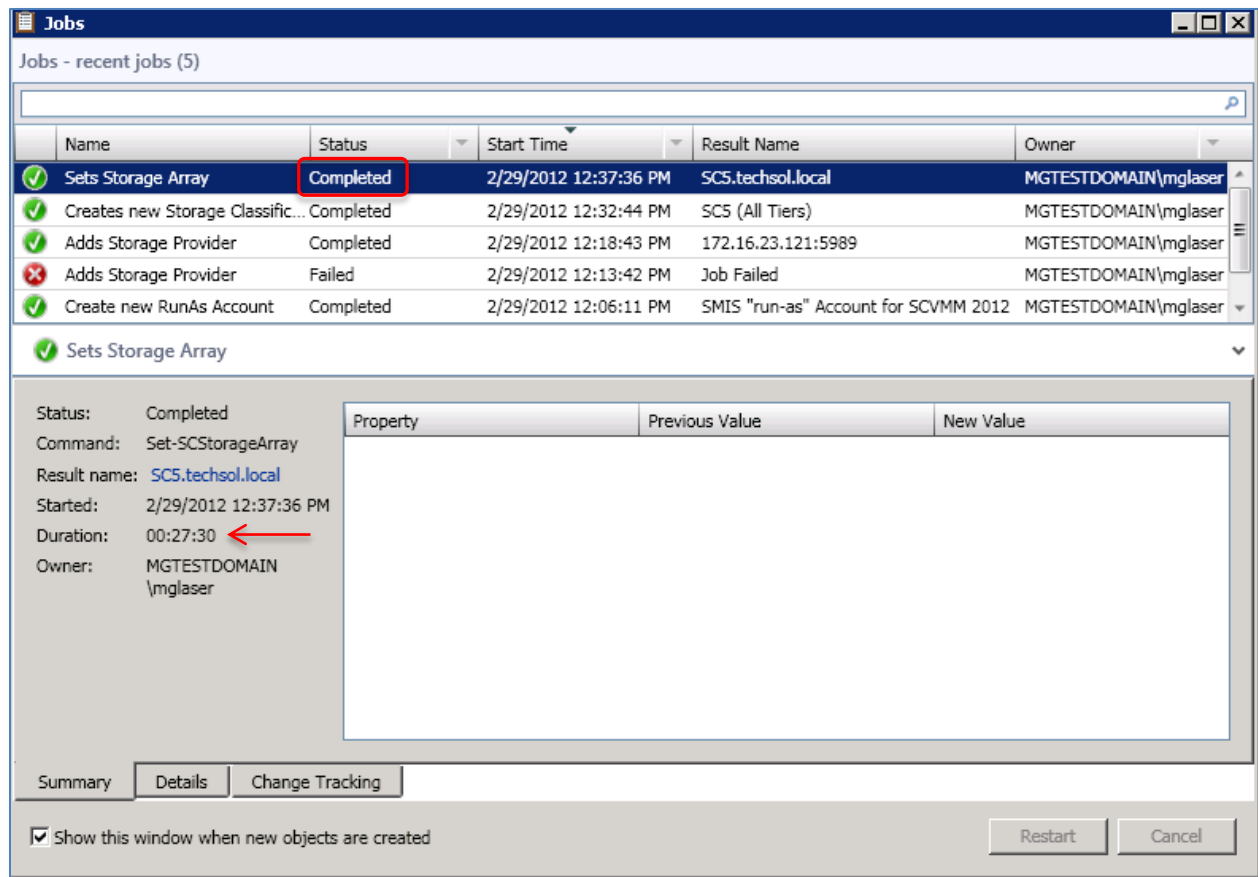


Figure 30: Successful completion of Sets Storage Array job

- 11) When the Sets Storage Array job finishes, the **Status** column should display a status of **Completed**. Note that the job in this example took 27.5 minutes as shown in Figure 30. Close out of the Jobs window.

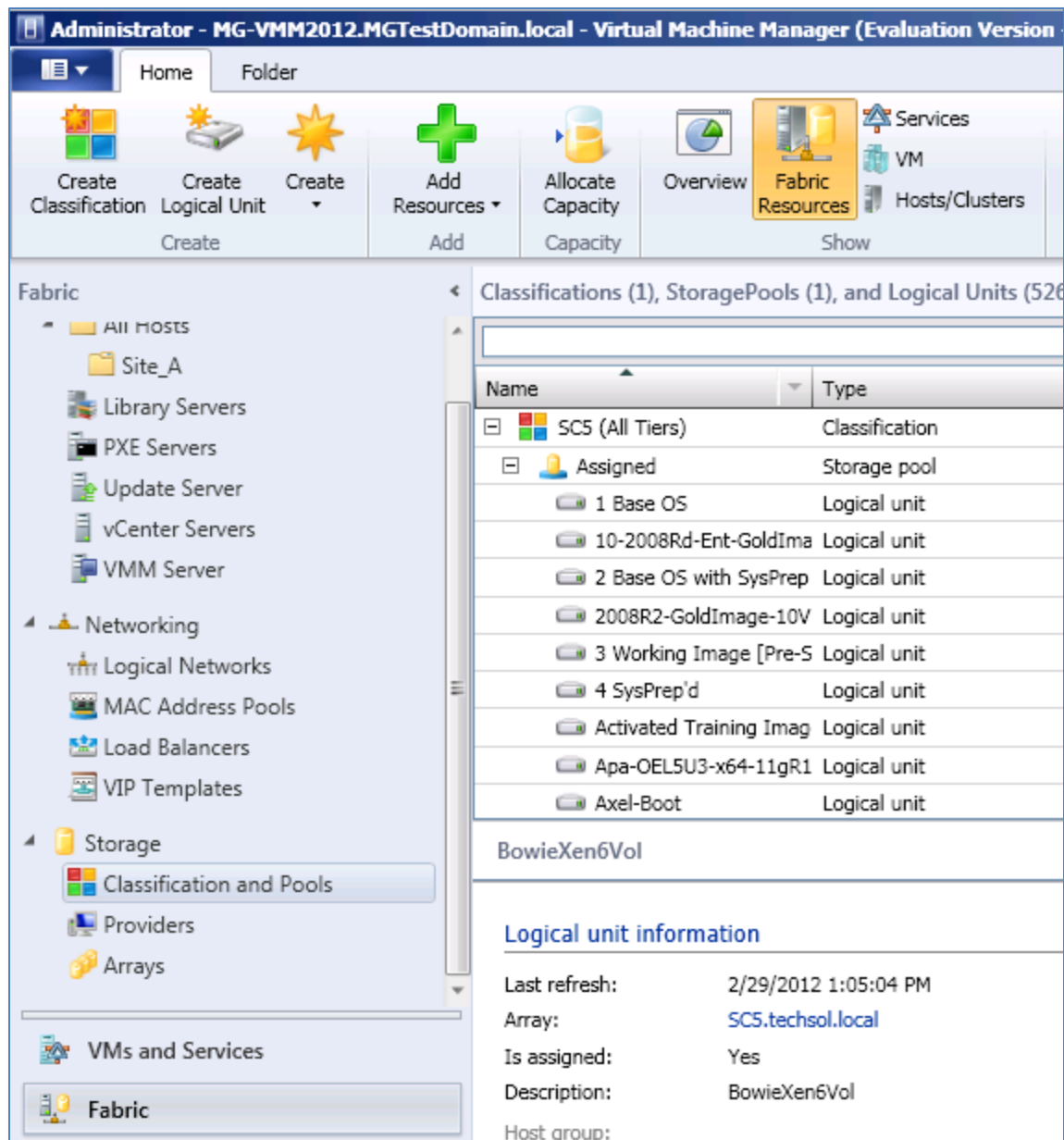


Figure 31: Storage pool assigned to a Classification

- 12) Under Classifications and Pools as shown in Figure 31, verify that the Storage Center volumes are now listed under the associated Storage Classification, **SC5 (All Tiers)** in this example. This Storage Center array can now be managed by SCVMM 2012.

Adding Additional Dell Compellent Storage Centers to SCVMM 2012

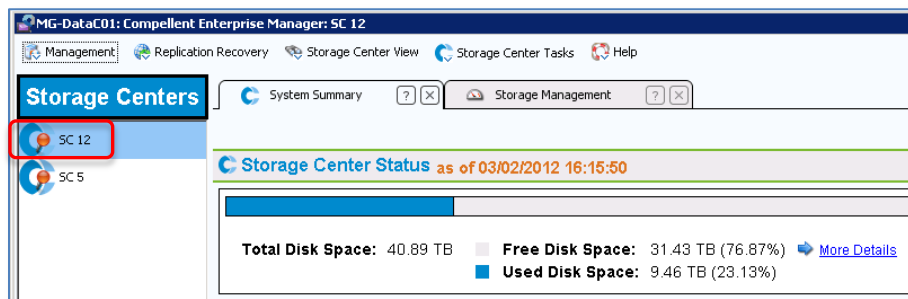


Figure 32: Additional Storage Center added to the Enterprise Manager client

- 1) If an additional Dell Compellent Storage Center needs to be managed by SCVMM 2012, then log in to the Enterprise Manager Client as the SMIS user and select **Add Storage Center** from the **Management** menu drop down. As shown in Figure 32 in this example, a second Storage Center named SC12 was added.

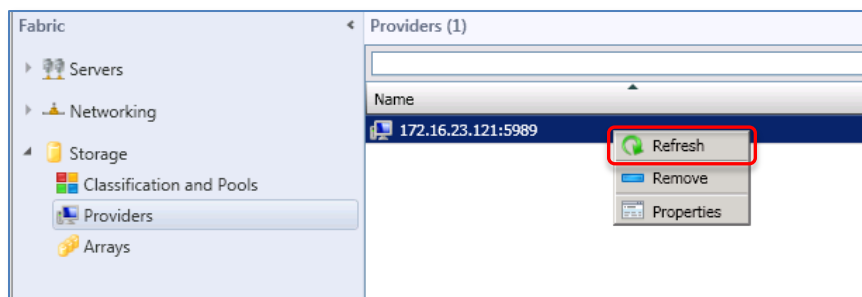


Figure 33: Discover an additional Storage Center by refreshing the Provider object

- 2) Once another Storage Center has been added to the Enterprise Manager Client, then using the SCVMM 2012 Administrator console, right-click on the storage provider object under Providers and click on **Refresh** as shown in Figure 33.

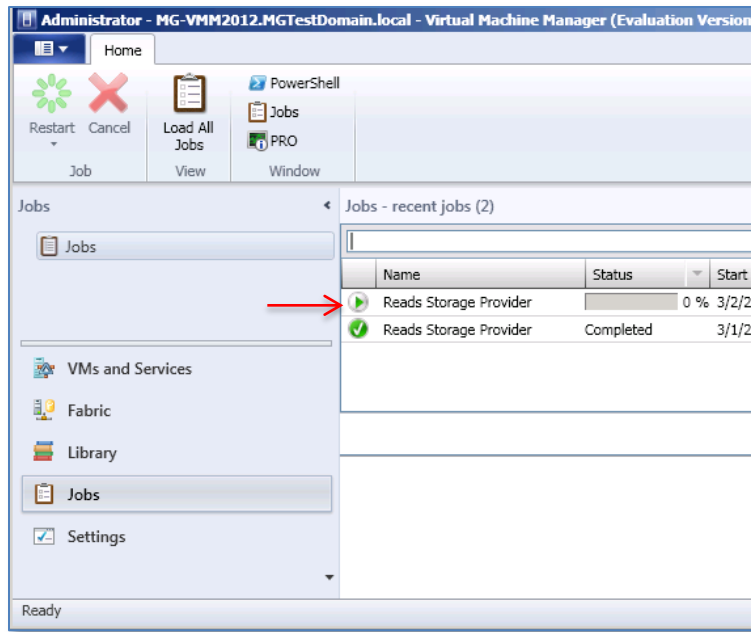


Figure 34: Monitor the Jobs screen until Reads Storage Provider Job finishes

- 3) Monitor the Jobs window in SCVMM 2012 until the **Reads Storage Provider** Job completes as shown in Figure 34. It may require up to 30 minutes or longer to finish.

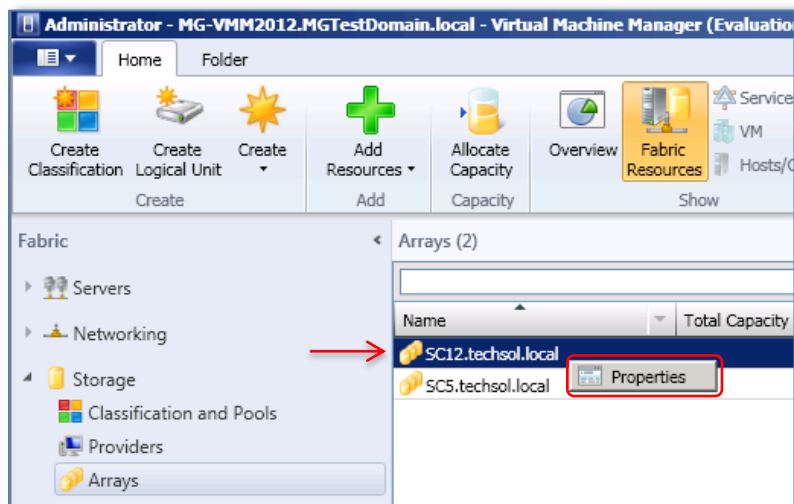


Figure 35: Additional Storage Center Array added to SCVMM 2012

- 4) Once the additional Storage Center has been discovered, it will be displayed as shown in Figure 35 under **Fabric**→ **Storage**→ **Arrays**. Right click on the new storage array and select **Properties**.

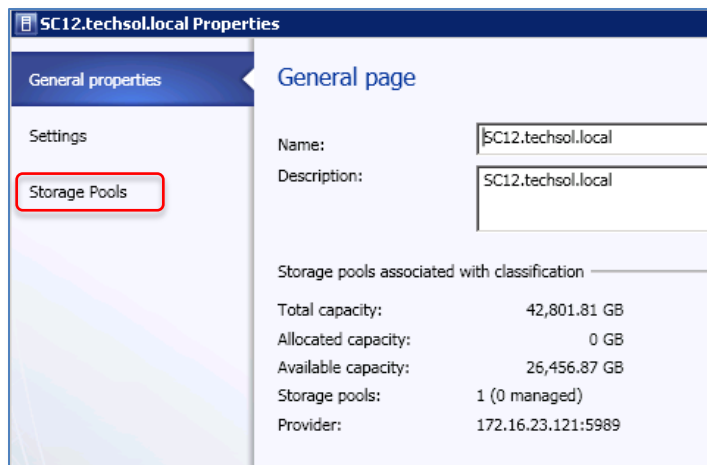


Figure 36: Storage Properties General page

5) On the Properties window, click on **Storage Pools** as shown in Figure 36.

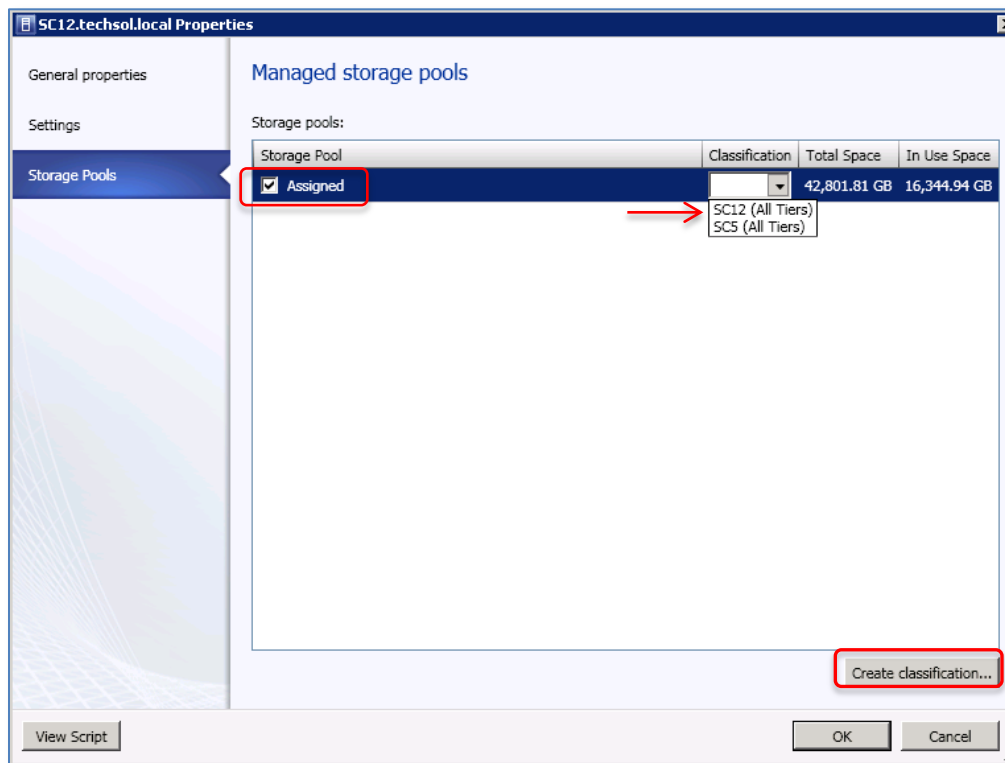


Figure 37: Create and assign a Classification to additional storage pool

6) On the Managed Storage Pools screen, check the box in front of **Assigned**. If necessary, create a new classification by clicking on the **Create Classification** button, or if the desired one already exists, choose it from the Classification drop-down list. In his example, a new Classification for SC12 was created and selected as shown in Figure 37. Then click on **OK**.

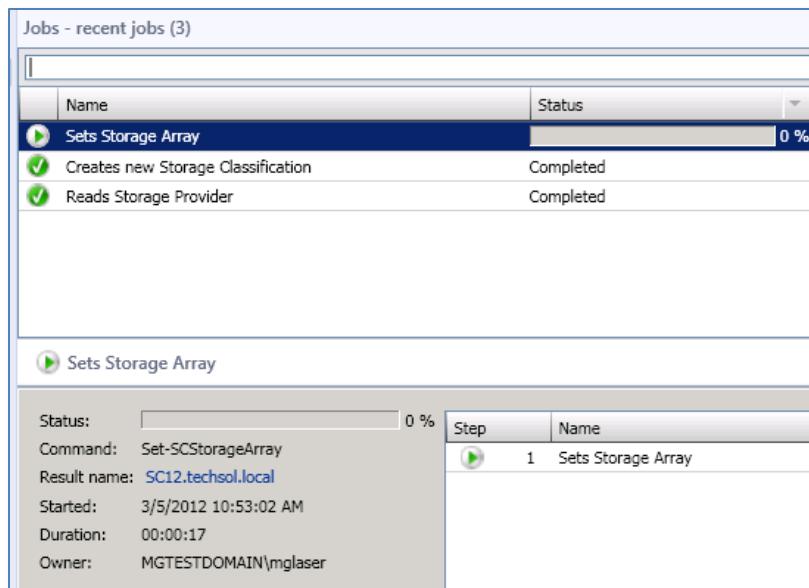


Figure 38: Sets Storage Array Job

- 7) Click on the Jobs in the left navigation pane, and monitor the **Sets Storage Array** job until it completes with a status of 100%. This may take up to 30 minutes or longer.

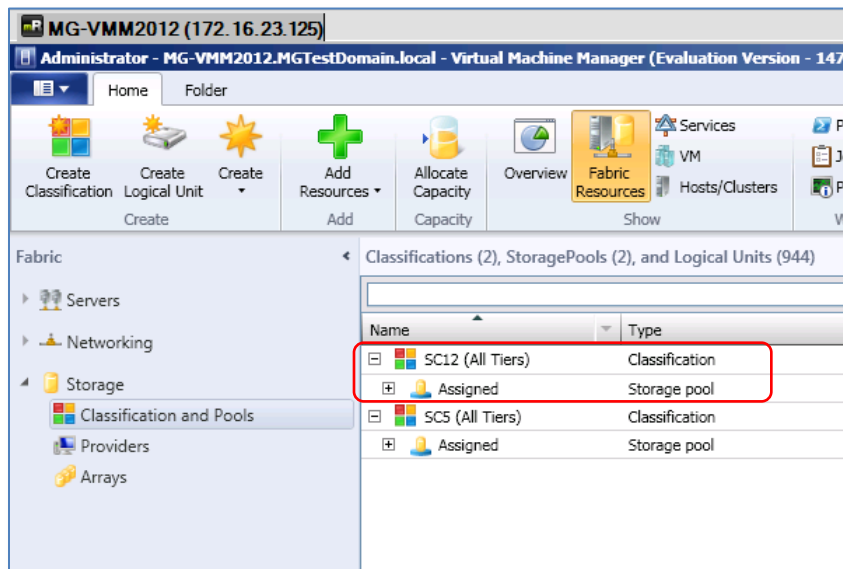


Figure 39: Classifications and Pools

- 8) Once the job has completed, click on **Fabric→ Storage→ Classifications and Pools**. The newly added storage array should now be listed under the Classification it was assigned to.

Name	Type
SC12 (All Tiers)	Classification
Assigned	Storage pool
__gui__WindowsSef5f9c	Logical unit
100linuxvms	Logical unit
1TBaixVxfsLV	Logical unit
500gbLVjfs2	Logical unit
50linuxvms	Logical unit
64tblun	Logical unit
Br-olt-11gR2-homeorac	Logical unit
Br-olt-11gR2-optoracleo	Logical unit
Camry_1	Logical unit

Figure 40: Volumes listed under an assigned storage pool

- 9) Click on the “+” in front **Assigned** and a list of existing volumes in the storage pool should be displayed as shown in Figure 39.

Classifications (3), StoragePools (3), and Logical Units (1070)	
Name	Type
SC12 (all tiers)	Classification
Assigned	Storage pool
SC13 (all tiers)	Classification
Assigned	Storage pool
SC5 (all tiers)	Classification
Assigned	Storage pool

Classifications (3), StoragePools (3), and Logical Units (1070)	
Name	Type
SC12 (all tiers)	Classification
SC12	Storage pool
SC13 (all tiers)	Classification
SC13	Storage pool
SC5 (all tiers)	Classification
SC5	Storage pool

Figure 41: Rename managed Storage Pools

- 10) For ease of management, if multiple Dell Compellent Storage Centers are managed as separate storage pools in SCVMM, then it is recommended that the **Assigned** object for each storage pool be renamed. To do so, right click on **Assigned** and edit the **Name** field under **Properties**. In the example shown in Figure 41, each instance of **Assigned** was changed to reflect the name of the associated Storage Center.

- 11) Repeat Steps 1 - 10 above to add additional Storage Centers to SCVMM 2012.



Multiple Dell Compellent Storage Centers can be discovered by SCVMM 2012 at the same time. However, assigning a classification to a discovered Storage Center in SCVMM should be done one at a time to avoid storage discovery failures.

Conclusion

Hopefully this document has proved helpful and has accomplished its purpose by providing administrators with answers to commonly asked questions associated with configuring the Dell Compellent SMI-S Provider 1.4 to work with Microsoft SCVMM 2012.

Appendix A: Manual creation of Local User Account on the Data Collector Server

If manual local Windows user creation is preferred on the Data Collector server, then follow the steps listed below. When completed, return to Page 18 above and run the PowerShell script to complete the creation of the OpenPegasus SMI-S user.

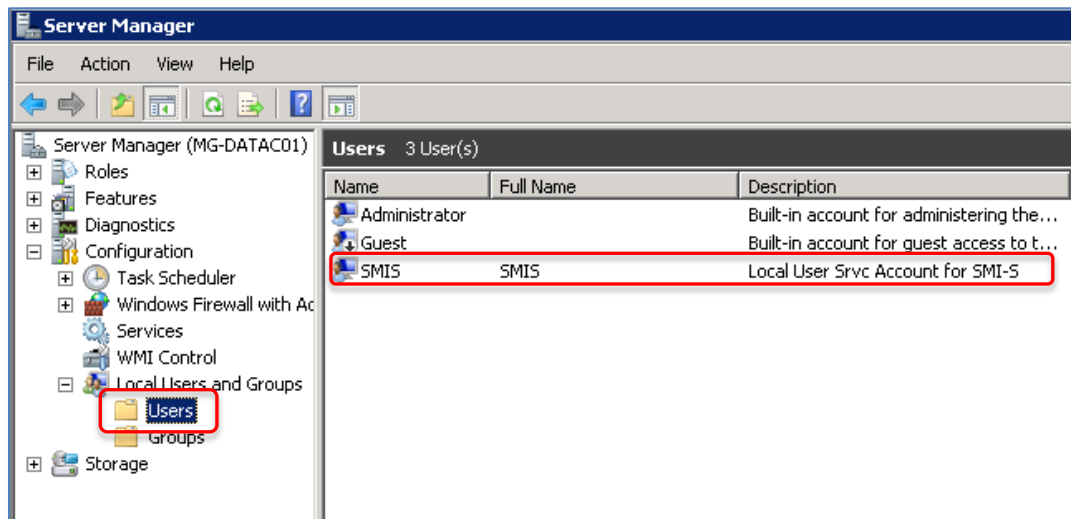


Figure 42: Create a local user account on the Data Collector server

- 1) On the Data Collector server, go to **Start → Administrative Tools → Server Manager**. In the **Users** folder under **Local Users and Groups**, create a local user account as shown in Figure 42. Provide a password that meets the minimum complexity requirements for your environment. For more information about user name and password requirements, see **Table 3**.

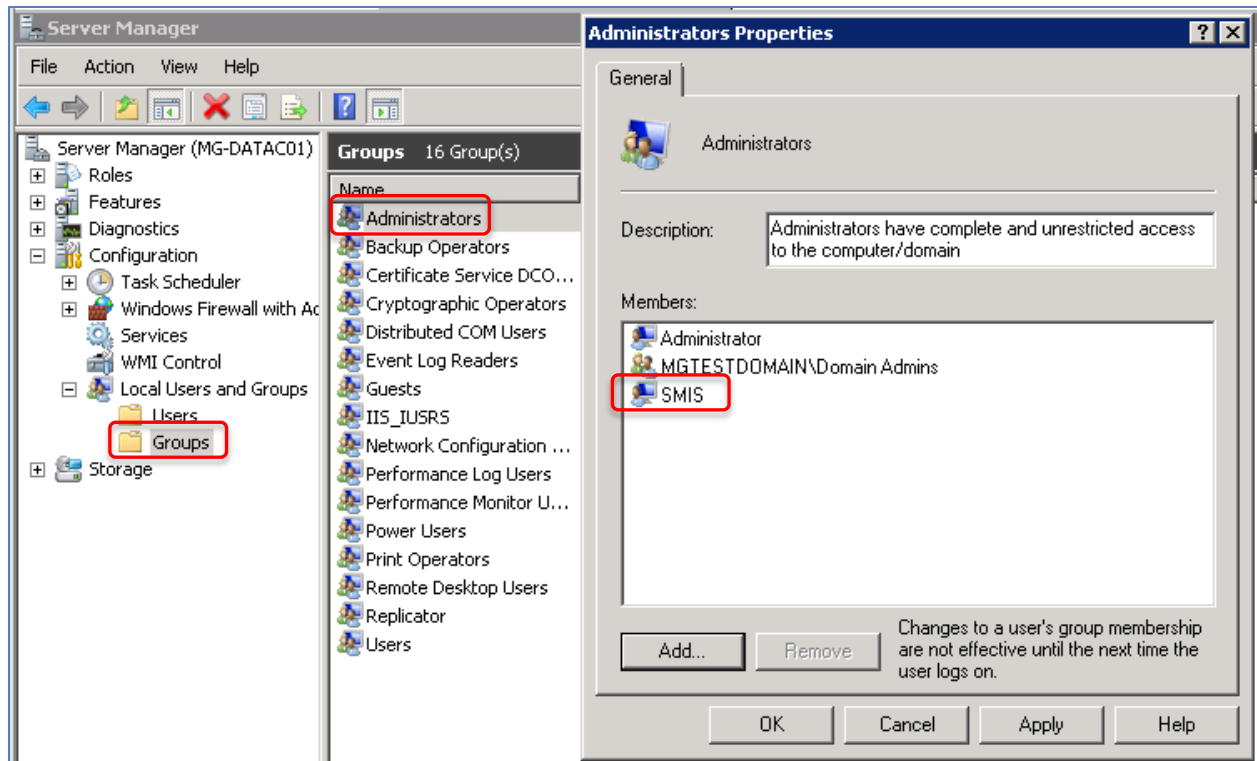


Figure 43: Add the local user to the local administrators group

- 2) As shown in Figure 43, once the local user has been created, add this new user to the local Administrators user group on the Data Collector server.

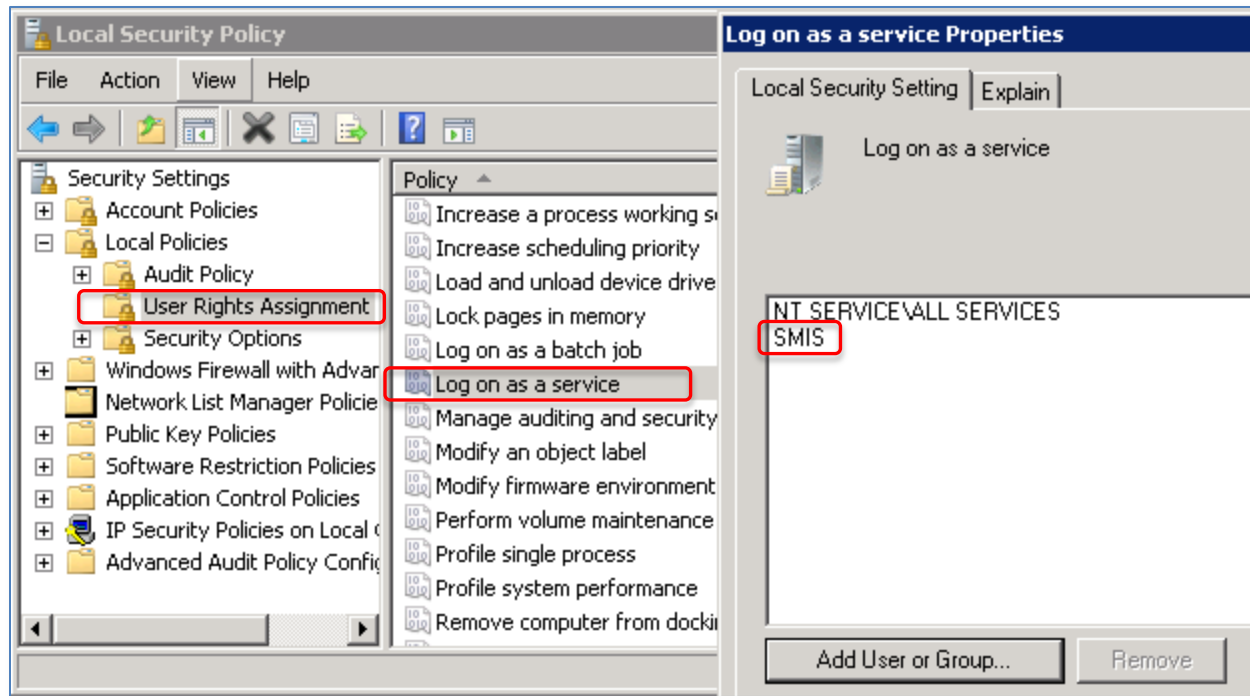


Figure 44: Grant local user the “Log on as a service” right

- 3) On the Data Collector server, go to **Start → Administrative Tools → Local Security Policy**. Expand **Local Policies**, and as shown in Figure 44, grant the local user the “Log on as a service” right under **User Rights Assignments**.
- 4) Return to Page 18 to run the PowerShell Script to create the OpenPegasus SMI-S User.