

ApplianceWatch PRO™ 2.1.1 for Microsoft® System Center Operations Manager **Release Notes**

NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089 U.S.A.
Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 4-NETAPP
Documentation comments: doccomments@netapp.com
Information Web: <http://www.netapp.com>

Part number: 215-05629_A0
(November) (2010)

Contents

Copyright information	5
Trademark information	7
New features in ApplianceWatch PRO 2.1.1	9
ApplianceWatch PRO 2.1.1 limitations	11
Documentation corrections and additions	13
SCVMM Self-Service Portal 2.0 installation and configuration considerations	13
Creating an action script for creating and deleting virtual machines	14
Windows Failover Clusters and cluster-shared volumes not supported	16
MetroCluster monitoring	16
Guidelines for using the MetroCluster TieBreaker Manager	17
Using the MetroCluster TieBreaker Manager	17
Reassembling a failed-over cluster	18
Known issues	19
Cmdlets need to map LUNs to igroups with type hyper_v only	19
PowerShell execution policy set to Allsigned causes New-Clone cmdlet to fail	20
New-Clone commandlet might leave free space	20
New-Clone commandlet fails on vFiler units using Data ONTAP versions earlier than 7.3.3	21
New-Clone commandlet fails to create virtual machine on clustered remote server	21
Running provisioning and cloning commandlets as a user other than built-in administrator	21
Uninstalling ApplianceWatch PRO	22
Removing the DeviceControlLibrary assembly after uninstallation	23
PRO discovery rules should run less frequently than monitoring rules	24
Restart of SCVMM SSP 2.0 might be required after installation or upgrade to ApplianceWatch 2.1.1	24
Default settings and timeouts in SCVMM SSP 2.0 might limit number of simultaneous CreateVM requests	24
ApplianceWatch installation execution results in error 1158:	25
Index	27

Copyright information

Copyright © 1994–2010 NetApp, Inc. All rights reserved. Printed in the U.S.A.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S.A. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

Trademark information

NetApp; the NetApp logo; the Network Appliance logo; Bycast; Cryptainer; Cryptoshred; DataFabric; Data ONTAP; Decru; Decru DataFort; FAServer; FilerView; FlexCache; FlexClone; FlexShare; FlexVol; FPolicy; gFiler; Go further, faster; Manage ONTAP; MultiStore; NearStore; NetCache; NOW (NetApp on the Web); ONTAPI; RAID-DP; SANscreen; SecureShare; Simulate ONTAP; SnapCopy; SnapDrive; SnapLock; SnapManager; SnapMirror; SnapMover; SnapRestore; SnapValidator; SnapVault; Spinnaker Networks; Spinnaker Networks logo; SpinAccess; SpinCluster; SpinFlex; SpinFS; SpinHA; SpinMove; SpinServer; SpinStor; StorageGRID; StoreVault; SyncMirror; Topio; vFiler; VFM; and WAFL are registered trademarks of NetApp, Inc. in the U.S.A. and/or other countries. Network Appliance, Snapshot, and The evolution of storage are trademarks of NetApp, Inc. in the U.S.A. and/or other countries and registered trademarks in some other countries. The StoreVault logo, ApplianceWatch, ApplianceWatch PRO, ASUP, AutoSupport, ComplianceClock, DataFort, Data Motion, FlexScale, FlexSuite, Lifetime Key Management, LockVault, NOW, MetroCluster, OpenKey, ReplicatorX, SecureAdmin, Shadow Tape, SnapDirector, SnapFilter, SnapMigrator, SnapSuite, Tech OnTap, Virtual File Manager, VPolicy, and Web Filer are trademarks of NetApp, Inc. in the U.S.A. and other countries. Get Successful and Select are service marks of NetApp, Inc. in the U.S.A.

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. A complete and current list of other IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.shtml.

Apple is a registered trademark and QuickTime is a trademark of Apple, Inc. in the U.S.A. and/or other countries. Microsoft is a registered trademark and Windows Media is a trademark of Microsoft Corporation in the U.S.A. and/or other countries. RealAudio, RealNetworks, RealPlayer, RealSystem, RealText, and RealVideo are registered trademarks and RealMedia, RealProxy, and SureStream are trademarks of RealNetworks, Inc. in the U.S.A. and/or other countries.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

NetApp, Inc. is a licensee of the CompactFlash and CF Logo trademarks.

NetApp, Inc. NetCache is certified RealSystem compatible.

New features in ApplianceWatch PRO 2.1.1

ApplianceWatch PRO 2.1.1 offers new features to assist you in monitoring the health of your Data ONTAP storage.

The following new features have been added to ApplianceWatch PRO 2.1.1:

- Script integration for Microsoft Virtual Machine Manager Self-Service Portal 2.0

In addition to the new features in ApplianceWatch PRO, you can also use the new rapid provisioning and cloning cmdlets to utilize Microsoft System Center Virtual Machine Manager applications.

ApplianceWatch PRO 2.1.1 also includes the following major new and enhanced features introduced in ApplianceWatch 2.1:

- Additional PRO Tips for managing virtual machines
- Improved health and monitoring diagnostics
- Reporting management pack so you can view reports on various aspects of your storage
- MetroCluster management pack for assistance during MetroCluster installation and help recovering from failover

ApplianceWatch PRO 2.1.1 limitations

Some features are not supported ApplianceWatch PRO 2.1.1.

The following features are not supported in ApplianceWatch PRO 2.1.1:

- Traditional volumes
- Data ONTAP GX and Data ONTAP 8.0 Cluster-Mode
- Pass-through disks
- Full support for high availability
- Adding or monitoring vFiler units (vFiler units added and monitored using partner vFiler units)
- Windows Failover Clusters and Cluster Shared Volumes (CSVs)
- SnapMirror source and destination storage controllers need to be monitored to generate SnapMirror replication-related PRO Tips and to view SnapMirror status
- Interacting with NetApp Operations Manager

Documentation corrections and additions

This section contains information that has been added or corrected.

Next topics

[*SCVMM Self-Service Portal 2.0 installation and configuration considerations*](#) on page 13

[*Creating an action script for creating and deleting virtual machines*](#) on page 14

[*Windows Failover Clusters and cluster-shared volumes not supported*](#) on page 16

[*MetroCluster monitoring*](#) on page 16

SCVMM Self-Service Portal 2.0 installation and configuration considerations

You can use Microsoft System Center Virtual Machine Manager Self-Service Portal 2.0 with the rapid provisioning and cloning cmdlets to facilitate virtual machine creation and deletion. The System Center Virtual Machine Manager Self-Service Portal does have requirements for use and you should have the necessary information available to assist you in installation and configuration.

The System Center Virtual Machine Manager Self-Service Portal calls the Rapid Provisioning PowerShell script included with the cmdlet installation and invokes the New-Clone cmdlet. The New-Clone cmdlet must run on the same host as the host on which the SCVMM library share is located. This is the host that contains the virtual machine template needed to create clones.

To install System Center Virtual Machine Manager Self-Service Portal, you must have the following information available:

- Domain user account with which the portal is installed (you can not use the local system account)
- Host name for the Web Service component
- Host name on which the SCVMM library share is located

To configure System Center Virtual Machine Manager Self-Service Portal 2.0, you must have the following information available:

- URL of Web portal
- SCVMM server name
- DHCP server FQDN
- SAN storage system information
- Network used by the virtual machines
- Active Directory Domain Names
- Quota cost
- SCVMM library server name
- SCVMM library share name

- Virtual machine templates from which you want to provision virtual machines
- Action scripts to copy into SCVMM Self-Service Portal

To configure the Rapid Provisioning PowerShell scripts, you can use the scripts from the following files:

- ONTAPCreateVM.txt
- ONTapCreateVMLocked.txt
- ONTapDeleteVM.txt
- ONTapDeleteVMLocked.txt

For more information on using System Center Virtual Machine Manager Self-Service Portal, see the Microsoft TechNet site.

Related information

Microsoft System Center - <http://technet.microsoft.com>

Creating an action script for creating and deleting virtual machines

You can use System Center Virtual Machine Manager Self-Service Portal 2.0 to extend CreateVM and DeleteVM actions by invoking the rapid provisioning PowerShell scripts. These extending actions enable you to use rapid provisioning quickly and more efficiently.

Before you begin

You must have met System Center Virtual Machine Manager Self-Service Portal 2.0 requirements and have configured it for use with the scripts. For more information on using System Center Virtual Machine Manager Self-Service Portal, see the Microsoft TechNet site.

Steps

1. In the Self-Service Portal, navigate to **Self Service Portal Settings > Customize Virtual Machine Actions > MasterActionXML**.
2. Select **CopyActionXML**.
3. Type the name for the new action script.

Example

For example, enter **ONTapRapidProvisioning**.

4. To create a virtual machine action, navigate to **CreateVM > Edit**.
5. Paste the ONTapCreateVM.txt content into the **Script** section of the edit window.
6. Paste the ONTapCreateVMLocked.txt content into the **LockedScript** section.

7. Set the options for the create action script.
 - a. For the Successful Return Code, enter 0.
 - b. Check the Timeout box and enter 9999.
 - c. Uncheck the Continue on Error box.
8. Click **Save and Close**.
9. To delete a virtual machine action, navigate to **DeleteVM > Edit**.
10. Paste the `ONTapDeleteVM.txt` content into the **Script** section of the edit window.
11. Paste the `ONTapDeleteVMLocked.txt` content into the **LockedScript** section.
12. Set the options for the delete action script.
 - a. For the Successful Return Code, enter 0.
 - b. Check the Timeout box and enter 9999.
 - c. Uncheck the Continue on Error box.
13. Click **Save and Close**.
14. Navigate to **Infrastructure > ServiceRole > Edit**.
15. From the Action XML drop-down list, select **ONTapRapidProvisioning**.

This step ensures the use of the script during the CreateVM or DeleteVM action. This script name must match the name you used to create the script.

Related information

Microsoft System Center - <http://technet.microsoft.com>

Windows Failover Clusters and cluster-shared volumes not supported

Although ApplianceWatch 2.1 and 2.1.1 require Windows Server 2008 R2 for installation and operation, not all features in Windows Server 2008 R2 are supported, including cluster-shared volumes (CSVs).

MetroCluster monitoring

ApplianceWatch PRO includes an optional MetroCluster management pack containing MetroCluster TieBreaker Manager and MetroCluster Recovery Assistant. These components monitor MetroCluster pairs and allow you to configure and initiate Cluster Failover on Disaster (CFOD) operations.

MetroCluster TieBreaker Manager

MetroCluster TieBreaker is a Windows service that you can install on the Microsoft System Center Operations Manager host server to monitor all discovered MetroClusters. MetroCluster TieBreaker detects failures that prevent a normal MetroCluster failover and forcibly trigger failover. You must enable this service manually after installation using the Windows Service Management utility. You can use MetroCluster TieBreaker Manager to determine which MetroCluster pairs you want to monitor and which conditions automatically trigger a failover.

MetroCluster Recovery Assistant

MetroCluster Recovery Assistant helps you reassemble a cluster after a Cluster Failover on Disaster event by directing you through the steps necessary to reestablish normal MetroCluster operation. After a disaster failover of a MetroCluster, you must rejoin and resynchronize the mirrored aggregates. This process can take several hours, during which MetroCluster Recovery Assistant displays the state of the cluster and the aggregate mirrors on each side as the operation progresses. You can use MetroCluster Recovery Assistant to manually initiate CFOD operations when the TieBreaker tool is not used or if it did not trigger a failover.

Next topics

[Guidelines for using the MetroCluster TieBreaker Manager](#) on page 17

[Using the MetroCluster TieBreaker Manager](#) on page 17

[Reassembling a failed-over cluster](#) on page 18

Guidelines for using the MetroCluster TieBreaker Manager

Before using the MetroCluster TieBreaker Manager, you must decide on a cluster poll interval and a recovery point objective, and you must enable fencing.

Cluster poll interval You can change the interval at which the TieBreaker service checks the health of a specific MetroCluster pair. The minimum interval is every 10 seconds, the maximum interval is every 600 seconds, and the default interval is every 30 seconds.

Recovery point objective A predetermined set of conditions must occur in a set period of time before a disaster failover can occur. These conditions include the inability to contact a member of the MetroCluster, the degradation of the root aggregate mirror on the remaining MetroCluster member, a cluster status of Error or Waiting, and the cluster interconnect being down. The recovery point objective (RPO) is the window of time during which all of the conditions must occur. The minimum interval is every 60 seconds, the maximum interval is every 4 hours, and the default interval is every 600 seconds.

Incorrect setting of the RPO interval can result in inconsistent data on the primary and disaster recovery copy. An automated failover under this condition leads to presenting stale data, which could cause the application to crash.

Fencing Before bringing a failed-over storage controller back online, you need to rejoin and resynchronize the aggregate mirrors in the MetroCluster to prevent possible data corruption. To do so, you can use the fencing option to fully power-down the failed-over storage controller using the remote LAN module (RLM) interface. The storage controller must contain RLM cards to use this option. If you use the fencing option and it fails, the tiebreaker service does not initiate disaster failover.

Using the MetroCluster TieBreaker Manager

You can use MetroCluster TieBreaker Manager to choose which MetroCluster pairs the TieBreaker service monitors, and to configure the conditions under which the TieBreaker service initiates the Cluster Failover on Disaster operation.

Before you begin

You must have imported and installed the MetroCluster management pack.

About this task

You should install the TieBreaker Manager on a System Center Operations Manager server at a separate location from either MetroCluster site, so that it operates as an objective arbiter of MetroCluster availability.

Steps

1. From the **Monitoring** pane, select **MetroClusters > State View**.

2. From the **Actions > Data ONTAP MetroCluster Pair Tasks** pane, select **MetroCluster TieBreaker Manager**.

The MetroCluster TieBreaker Settings dialog box opens.

3. Select the MetroCluster pair for which you want to configure the tiebreaker service.
4. To enable tiebreaker features, click the **Enable TieBreaker** check box.
5. (Optional) Change the value in the **Cluster poll interval** box.
6. (Optional) Change the value in the **Recovery point objective** box.
7. (Optional) Click the **Require Fencing** check box.
8. Enter the RLM user name and password for each of the cluster members.
9. Click **Apply** and then click **OK**.

Result

The parameters are saved into the Microsoft System Center Operations Manager database. The TieBreaker service reads the parameters every 15 minutes and updates operations as necessary.

Reassembling a failed-over cluster

You can use the MetroCluster Recovery Assistant to assist you in reassembling a cluster after it has failed over. You can also view the status of a MetroCluster and its mirrored aggregates or manually initiate a Cluster Failover on Disaster event.

Before you begin

You must have imported and installed the MetroCluster management pack.

Steps

1. From the **Monitoring** pane, select **MetroClusters > State View**.
2. Select the MetroCluster you want to recover.
3. From the **Actions > Data ONTAP MetroCluster Pair Tasks** pane, select **MetroCluster Recovery Assistant**.

The MetroCluster Recovery Assistant dialog box opens.

4. Click **Help** and follow the steps to restore the MetroCluster to normal operation.

Known issues

This section contains the known issues for this release of ApplianceWatch PRO.

Next topics

- [*Cmdlets need to map LUNs to igroups with type hyper_v only*](#) on page 19
- [*PowerShell execution policy set to Allsigned causes New-Clone cmdlet to fail*](#) on page 20
- [*New-Clone commandlet might leave free space*](#) on page 20
- [*New-Clone commandlet fails on vFiler units using Data ONTAP versions earlier than 7.3.3*](#) on page 21
- [*New-Clone commandlet fails to create virtual machine on clustered remote server*](#) on page 21
- [*Running provisioning and cloning commandlets as a user other than built-in administrator*](#) on page 21
- [*Uninstalling ApplianceWatch PRO*](#) on page 22
- [*Removing the DeviceControlLibrary assembly after uninstallation*](#) on page 23
- [*PRO discovery rules should run less frequently than monitoring rules*](#) on page 24
- [*Restart of SCVMM SSP 2.0 might be required after installation or upgrade to ApplianceWatch 2.1.1*](#) on page 24
- [*Default settings and timeouts in SCVMM SSP 2.0 might limit number of simultaneous CreateVM requests*](#) on page 24
- [*ApplianceWatch installation execution results in error 1158:*](#) on page 25

Cmdlets need to map LUNs to igroups with type hyper_v only

If you use the New-Storage, Connect-Storage, or New-Clone cmdlets to map LUNs to igroups with a type other than hyper_v, you will receive an error. This applies only to igroups containing host initiators.

To successfully run LUN mapping to the host initiator task, you must change the igroup type to hyper_v. If you have mapped any other LUNs to igroups with a type other than hyper_v, you must first delete the mappings and then change the type to hyper_v. If you have not mapped any LUNs to igroups with a type other than hyper_v, you can delete the igroup and retry the operation.

PowerShell execution policy set to Allsigned causes New-Clone cmdlet to fail

If you use the recommended PowerShell Allsigned execution policy with the New-Clone cmdlet, it will fail. You can import the Microsoft System Center Virtual Machine Manager certificate as a Trusted Publisher to avoid this error.

There is a dependency in the SCVMM PowerShell cmdlets to retrieve the list of virtual machines. To allow retrieval using the recommended execution policy of Allsigned, you must import the SCVMM certificate. For more information on importing a certificate, see the Microsoft Web site.

Related information

<http://www.microsoft.com>

New-Clone commandlet might leave free space

The New-Clone commandlet might leave free space when creating or cloning a new LUN for a virtual machine. If the free space is larger than 8 MB, it shows up in Disk Management.

When you create or clone the LUN, the full space is not used in the partitioning and formatting of the LUN. You can leave the space as it is, and the commandlet still performs correctly.

New-Clone commandlet fails on vFiler units using Data ONTAP versions earlier than 7.3.3

The use of vFiler units is only supported when using Data ONTAP version 7.3.3.

New-Clone commandlet fails to create virtual machine on clustered remote server

Even though cloning is not supported in cluster-shared volume and clustered environments, you do not receive an error immediately. The commandlet executes the operation and then fails when creating the virtual machine.

Running provisioning and cloning commandlets as a user other than built-in administrator

You can avoid running the rapid provisioning and cloning commandlets as the built-in Windows administrator and run them as a user in the Administrators group.

Before you begin

You must have installed the rapid provisioning and cloning commandlets.

Steps

1. Open the Windows **Start** menu.
2. Select **Run** and type `secpol.msc` and click **OK**.
3. From the **Local Security Settings** window, click **Local Policies** and then **Security Options**.
4. Double-click **User Account Control: Run all administrators in Admin Approve Mode**.
5. Select **Disabled** and click **OK**.
6. Close the **Local Security Settings** window.
7. Restart the Windows host.

Result

After you restart the Windows 2008 R2 server, you can run the rapid provisioning and cloning commandlets without being the Windows built-in administrator.

Uninstalling ApplianceWatch PRO

You can cleanly remove ApplianceWatch PRO 2.0 or ApplianceWatch 2.1 from Microsoft System Center Operations Manager and re-import them.

Before you begin

You must have installed ApplianceWatch PRO 2.0 or ApplianceWatch 2.1 and imported the management packs into Microsoft System Center Operations Manager.

Steps

1. Navigate to **SCOM > Administration > Management Packs > Import Management Packs**.
2. Type **ONTAP** in the search box and click **Find Now**.
3. Right-click each of the four management packs and select **Delete**.
Note: System Center Operations Manager might prompt you to remove the default management pack. You can remove it and reinstall it after you have uninstalled ApplianceWatch.
4. To remove the default management pack, navigate to **SCOM > Administration > Management Packs > Import Management Packs**.
5. Type **Default** in the search box and click **Find Now**.
6. Right-click **Default Management Pack** and select **Delete**.
7. Close System Center Operations Manager.
8. Uninstall the ApplianceWatch PRO management packs. For more information, see the *ApplianceWatch PRO 2.1 for Microsoft System Center Operations Manager Installation and Administration Guide*.
9. To re-import the default management pack, navigate to **SCOM > Administration > Management Packs > Import Management Packs**.
10. Select **Add > Add from disk** and locate the C:\Program Files\System Center Operations Manager 2007 folder.
11. Select the `Microsoft.SystemCenterOperationsmanager.DefaultUser` file and click **Install**.
Even if you choose not to install ApplianceWatch PRO 2.1, you must re-import the default SCOM management pack.
12. Re-import the ApplianceWatch PRO 2.1 management packs. For more information, see the *ApplianceWatch PRO 2.1 for Microsoft System Center Operations Manager Installation and Administration Guide*.

13. Add the Data ONTAP storage controllers and set credentials. For more information, see the *ApplianceWatch PRO 2.1 for Microsoft System Center Operations Manager Installation and Administration Guide*.

You must set the target type to Management Server for the Data ONTAP settings to appear in the Actions pane.

Related information

<http://now.netapp.com/NOW/>

Removing the DeviceControlLibrary assembly after uninstallation

Upon uninstallation, ApplianceWatch PRO 2.1 leaves the DeviceControlLibrary assembly in the Windows Global Assembly Cache (GAC). You can remove this file to clean up after the uninstallation.

Before you begin

You must have uninstalled ApplianceWatch PRO 2.1.

Steps

1. In the c:\Windows\assembly folder, locate **DeviceControlLibrary**.
2. Right-click **DeviceControlLibrary** and select **Uninstall**.

The assembly is removed from the Windows GAC.

PRO discovery rules should run less frequently than monitoring rules

You should not change the default values of discovery rules, but if you do change them, they should run less frequently than the monitoring rules.

Restart of SCVMM SSP 2.0 might be required after installation or upgrade to ApplianceWatch 2.1.1

You should restart Microsoft System Center Virtual Machine Manager Self-Service Portal 2.0 after installation or upgrade to refresh its knowledge of environmental variables that point to the ApplianceWatch PRO 2.1.1 installation folder.

Default settings and timeouts in SCVMM SSP 2.0 might limit number of simultaneous CreateVM requests

Microsoft System Center Virtual Machine Manager Self-Service Portal 2.0 service and portal have different timeout settings that might affect the success of a large number of CreateVM requests.

You can use the following settings to enable you to create large numbers of CreateVM requests:

- Portal setting - sessionState timeout
- Service setting - maxSimultaneousWorkflows
- Service setting - maxVMHostCapacity

To change the settings or timeouts, see the following Microsoft documentation:

- Virtual Machine Manager Self-Service Portal Operations Guide
- Virtual Machine Manager Self-Service Portal Administration Guide
- Virtual Machine Manager Self-Service Portal Deployment Guide
- Virtual Machine Manager Self-Service Portal Extensibility Guide

After changing the settings, you should restart the Self-Service Portal.

Related information

<http://www.microsoft.com>

ApplianceWatch installation execution results in error 1158:

When you start the installation from the package executable, a pop-up error message might appear with just the error number "1158." You can retry the installation and the problem should be resolved.

If the problem persists, close any unnecessary windows that are open on the desktop. You can go to **Control Panel > Uninstall** and refresh the list of programs. You can retry the installation and the error message should be resolved.

Index

A

ApplianceWatch PRO 9, 11
 limitations 11
 new features 9

G

guidelines 17
 before using the MetroCluster TieBreaker Manager
 17

K

Known issues 19

L

limitations 11

ApplianceWatch PRO 11

M

MetroCluster TieBreaker Manager 17
 guidelines 17
 using 17

N

new features 9

U

using 17
 MetroCluster TieBreaker Manager 17

