Access Control Policies

The new feature within EqualLogic firmware 7.0 that enables centralized management of access controls for volume access.

Dell Engineering
January 2014

This document has been archived and will no longer be maintained or updated.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.
Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>January 2014</td>
<td>Initial release</td>
</tr>
</tbody>
</table>

THIS WHITE PAPER 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.

© 2013 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. PRODUCT WARRANTIES APPLICABLE TO THE DELL PRODUCTS DESCRIBED IN THIS DOCUMENT MAY BE FOUND AT: [http://www.dell.com/learn/us/en/19/terms-of-sale-commercial-and-public-sector](http://www.dell.com/learn/us/en/19/terms-of-sale-commercial-and-public-sector) Performance of network reference architectures discussed in this document may vary with differing deployment conditions, network loads, and the like. Third party products may be included in reference architectures for the convenience of the reader. Inclusion of such third party products does not necessarily constitute Dell’s recommendation of those products. Please consult your Dell representative for additional information.

Trademarks used in this text:

Dell™, the Dell logo, Dell Boomi™, Dell Precision™, OptiPlex™, Latitude™, PowerEdge™, PowerVault™, PowerConnect™, OpenManage™, EqualLogic™, Compellent™, KACE™, FlexAddress™, Force10™ and Vostro™ are trademarks of Dell Inc. Other Dell trademarks may be used in this document. Cisco Nexus®, Cisco MDS®, Cisco NX-OS®, and other Cisco Catalyst® are registered trademarks of Cisco System Inc. EMC VNX®, and EMC Unisphere® are registered trademarks of EMC Corporation. Intel®, Pentium®, Xeon®, Core® and Celeron® are registered trademarks of Intel Corporation in the U.S. and other countries. AMD® is a registered trademark and AMD Opteron™, AMD Phenom™ and AMD Sempron™ are trademarks of Advanced Micro Devices, Inc. Microsoft®, Windows®, Windows Server®, Internet Explorer®, MS-DOS®, Windows Vista® and Active Directory® are either trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. Red Hat® and Red Hat® Enterprise Linux® are registered trademarks of Red Hat, Inc. in the United States and/or other countries. Novell® and SUSE® are registered trademarks of Novell Inc. in the United States and other countries. Oracle® is a registered trademark of Oracle Corporation and/or its affiliates. Citrix®, Xen®, XenServer® and XenMotion® are either registered trademarks or trademarks of Citrix Systems, Inc. in the United States and/or other countries. VMware®, Virtual SMP®, vMotion®, vCenter® and vSphere® are registered trademarks or trademarks of VMware, Inc. in the United States or other countries. IBM® is a registered trademark of International Business Machines Corporation. Broadcom® and NetXtreme® are registered trademarks of Broadcom Corporation. Qlogic is a registered trademark of QLogic Corporation. Other trademarks and trade names may be used in this document to refer to either the entities claiming the marks and/or names or their products and are the property of their respective owners. Dell disclaims proprietary interest in the marks and names of others.
# Table of contents

Revisions ................................................................................................................................. 2  
Executive summary .................................................................................................................. 4  
1 Introduction .......................................................................................................................... 5  
2 Access policies user interface .............................................................................................. 6  
3 Volume access control usage and use cases ......................................................................... 7  
   3.1 Creating an access policy ............................................................................................... 7  
   3.2 Creating and modifying an access policy group .............................................................. 8  
   3.3 Assigning an access policy or access policy group to a volume .................................... 10  
   3.4 Assigning a basic access point (previously ACL) to a volume ....................................... 12  
   3.5 Migrating existing volumes to an access policy or access policy group ....................... 13  
   3.6 Copying access controls from another volume ............................................................... 13  
4 Limits ................................................................................................................................... 15  
5 Host Integration Toolkit compatibility ................................................................................... 16  
6 Glossary ............................................................................................................................... 17
Executive summary

In today’s ever changing dynamic data centers, flexibility and ease of use are key to efficient operation and meeting demands. Tasks that can be automated must be automated in order to free administrators for the more labor intensive tasks. For the tasks that cannot be automated, templates, procedures and policies provide a predefined means to meet company standards.

Dell EqualLogic has a long history of easy to use products and continues to maintain that reputation with each new innovation. The EqualLogic access control policies centralize access controls for volumes and make the process of establishing access for a new volume easier, quicker and less error prone. This enables IT to meet the growing demands of business needs.
Introduction

The ability for a server to access a particular volume on an EqualLogic SAN is restricted by the volume access controls. Controls are vital for the integrity of the data, as serious issues can arise if any server can access any volume. With iSCSI, this access control is achieved through the use of either one or a combination of:

- The host iSCSI initiator iSCSI Qualified Name (IQN)
- The IP address the server is using for iSCSI access
- CHAP (Challenge-Handshake Authentication Protocol)

This ensures that only the needed servers have access to specific volumes.

Prior to access control policies, access control to a volume was granted through the use of an access control list (ACL) entry, which are now referred to as basic access points. The traditional ACL was limited to defining access to a single volume. However, servers typically access multiple volumes. As a result, each volume required an identical, but separately managed ACL to control access from one server. If a cluster of servers needed to access a volume, as is often the case in present-day data centers, an additional ACL was required for each server in the cluster. When the environment grew, and a cluster required an additional volume, the new volume had to be configured with its own ACL (identical to the existing ACL) for the other volumes used by the same cluster. An existing volume ACL could not be reused.

The EqualLogic firmware version 7.0 access control policies enable storage administrators to define access controls for multiple volumes in a simple manner. Storage administrators have the option of defining access for a particular server using an access policy, or grouping several of these policies together to define access for a cluster of servers, known as an access policy group.

When the environment grows and a new volume is required, the task of defining access is reduced to selecting the appropriate access policy or access policy group from the list of available policies when the volume is created. When a new server is added to a cluster, and its access policy has been added to the cluster’s access policy group, it automatically obtains access to all volumes defined for an access policy group. In either case, adding hardware to the environment becomes easier, less likely to produce errors and quicker to perform.
Access policies user interface

The access controls for all volumes on the array, along with the creation and modification of access policies and access policy groups can be centrally managed from the Access Policies tab under Group Configuration in the array web UI, as shown in the screenshot below.

In this example, an environment has been configured with multiple access policies and access policy groups. One of these access policy groups is labeled VirtualizationCluster, and contains three access policies labeled host-121, host-122, and host-123, each of which contains one extended access point configured with an IQN. The Targets pane displays the five volumes to which the access policy group VirtualizationCluster has been associated to: Virtualization01 thru Virtualization05. This information shows that the user has three servers in a clustered configuration utilizing five volumes for shared storage.

---

1. Extended access point: This is comparable to a basic access point or classic access control list (ACL) entry, in that it defines the CHAP account, iSCSI initiator name or IP addresses used for access control. An extended access point cannot be assigned to a volume.
2. Access policy: It consists of one or more extended access points and can be attached to multiple volumes and/or snapshots to control access to them.
3. Access policy group: It consists of one or more access polices and can be attached to multiple volumes and/or snapshots to control access to them.
4. A list of volumes, or targets, assigned to the selected access policy or access policy group.

Dell recommends using individual access policies for individual servers, and access policy groups for server clusters. This, coupled with providing logical names to the policies, provides clear and flexible volume access control management.
3 Volume access control usage and use cases

There are two different use cases when it comes to volume access controls; either the volume is to be accessed by one server, or it is to be accessed by a cluster of servers. However, these two use cases can be applied in various ways, and implemented using different methods. The examples provided below are not intended to be exhaustive in their coverage of all methods, but rather, provide examples of how and when the different methods can be used. As with many things in information technology, the best way of doing something is going to depend on the environment and its standard operating procedures.

The access control policy examples in this section use the following concepts: Access policies are used to control access from a single server and access policy groups are used to grant access from a cluster of servers. An access policy group is a collection of multiple access policies. Finally, Section 3.4 is an example of using basic access points as an update to the access control lists in prior releases.

3.1 Creating an access policy

The following steps explain how to create an access policy used to define access for a single server. It can be applied to one or more volumes.

2. In the New Access Policy dialogue box, provide a policy name. Populating the Description field is optional. Click New to create an extended access point.

3. On the New Extended Access Point dialogue box, supply at least one of the following to represent the server that will gain access:
   CHAP Account Name, iSCSI Initiator Name, or IP Addresses.

   In this example, the iSCSI initiator name was used.

4. Click OK.
If the extended access point is created with an iSCSI initiator name, and the server contains multiple HBA or hardware iSCSI initiators, then multiple extended access points will need to be added to the Access Policy.

If it is created using an IP Address, and multiple network cards are used in the server for iSCSI traffic, then either multiple extended access points need to be added to the access policy, or multiple IP addresses need to be added to one extended access point.

5. Click OK to close the New Access Policy dialogue box.

The access policy is complete and is available to provide volume access control for an individual server, and can be applied to new or existing volumes in the PS Group.

3.2 Creating and modifying an access policy group

In the previous example, an access policy for an individual server was created. In many datacenter environments, multiple servers provide high availability support for an application, or are used as hypervisor hosts for virtual machines. In these instances multiple servers, or a cluster of servers, all access the same volume or volumes.

To simplify volume access control management for cluster accessing several volumes, multiple access policies representing multiple servers in the cluster are combined into one access policy group. This access policy group (instead of individual access policies) is then applied to the volume (or volumes) that the cluster of servers will utilize. As servers are added to the cluster, the access control information associated with multiple volumes does not need to be changed. Instead, when a new server is added to the cluster, simply create an access policy for it and add it to the cluster’s access policy group. At that
point the new server will gain access to all the volumes to which the access group policy has been assigned.

This example explains the process for creating an access policy group, and also for modifying the access policy group to add access policies.

6. From the **Access Policies** tab in the **Group Configuration** window click **New** in the **Access Policies** pane.
7. In the **New Access Policy Group** dialogue box, provide a name, and optionally a description, as shown below.

![New Access Policy Group](image1)

8. The access policy, **host-124**, that was created in the previous example now be added to this access policy group. To start the process click **Add**.
9. The **Add Access Policies** dialog box displays all of the access policies that are configured on the array and are not a part of this access policy group. Select the **host-124** access policy that was created in the previous example, and the three other access policies with the description **Virtualization Cluster (host-121 thru host-123)**, and then click **OK**.

![Add Access Policies](image2)
This completes the creation of the VirtualizationCluster access policy group. It can be assigned to new or existing volumes in the PS Group.

Quite often, IT environments grow and change. Existing access group policies can easily be modified to respond to these changes. New access policies can be added to provide access for new servers in the cluster, and existing access policies can be removed as servers are decommissioned. To add or remove an access policy from an existing access policy group, follow the steps below.

1. Select an access policy group to change, and then click Modify.
2. From the Modify Access Policy Group dialogue box:
   a. To include another access policy in the access policy group, click Add. This launches the Add Access Policy dialogue box as seen in the previous example.
   b. To remove an access policy, select the access policy and click Remove.
3. Once the additions, modifications, or removals are complete, click OK to finish the process.

### 3.3 Assigning an access policy or access policy group to a volume

One benefit of the new access controls feature is that the process of assigning access controls to a volume is easier; particularly where multiple servers are involved. Where the task previously involved a number of repetitive steps, it has been reduced to simply selecting the appropriate predefined access policy or access policy group from a list. This example demonstrates assigning access controls to a new volume during the volume creation process.

1. From the Volumes page, click the Create Volume link.
2. Provide a Name for the volume, and click Next.
3. Specify a size for the new volume, and click Next.
4. During this step in the volume creation process, select the volume access controls. As shown in the screenshot below, there are a number of options available.
In this example, **Select or define access control policies** is selected. The first option is covered in **Section 3.4**, and the third option in **Section 3.6**. The forth option (None) permits the creation of volumes without immediately defining access; which can be done at a later point.

5. Select the radio box for **Access Policies** or **Access Policy Groups**, and then select the relevant policy for the volume. In this example, the access policy group **VirtualizationCluster** is selected. Click **Add**.

   It is possible to apply multiple access policies or access policy groups to a single volume. One use case would be to share out a volume used to store installation media ISOs among multiple virtualization clusters.

6. Click **Next** to continue.

   **Note:** if the volume is to be accessed by multiple iSCSI initiators, set the **Do you want to allow simultaneous access to this volume from more than one iSCSI initiator?** radio button to **Yes**.

   7. Select the appropriate sector size, and click **Next** to continue.
   8. The final dialog box in the create volume process displays a summary of the options selected. Verify that the options are correct, and click **Finish** to create the volume.

In this example the process for creating a volume and assigning access controls using access policies or access policy groups was explained. This enabled assigning access controls from a predefined list of policies without the risk of mistyping an IQN or IP address. In addition, access was granted to multiple servers defined by the **VirtualizationCluster** access policy group.
3.4 Assigning a basic access point (previously ACL) to a volume

While there are many benefits to using access control policies, it is possible to continue to use an ACL for assigning volume access control. The current name for this functionality is basic access point. The process for assigning and modifying a basic access point to a volume is largely unchanged.

1. From the Volumes page, click Create Volume.
2. Provide a Name for the volume, and click Next.
3. Specify the volume size, and click Next.
4. During this step in the volume creation process, that the volume access controls are defined. As shown in the screenshot below, there are a number of options available.

![Create Volume Screenshot]

In this example, Define one or more basic access points is selected. Click Add to continue.

5. In the New Basic Access Point dialog box, enter in the CHAP account name, iSCSI initiator name or IP address, for controlling access to the volume, and then click OK. If multiple iSCSI initiator names or IP addresses are required, add additional Basic Access Points.

**Note:** If the volume is to be accessed by multiple iSCSI initiators set the “Do you want to allow simultaneous access to this volume from more than one iSCSI initiator?” radio button to Yes.

6. Select the appropriate sector size, and click Next to continue.
7. The final dialog box in the create volume process displays a summary of the selected options. Verify that the options are correct, and click Finish to create the volume.
3.5 Migrating existing volumes to an access policy or access policy group

This section covers the steps needed to migrate a volume using basic access points to using an access control policy without disruption.

Access control policies provide several benefits. Primarily, it is significantly easier to manage volume access controls for clustered servers. In addition, they provide an increase in the number of access control records that can be assigned to an individual volume and to the environment as a whole.

It is important to note that this section is intended to provide guidance for the process, and is not intended as a thorough end to end decision making or as a troubleshooting guide. It is strongly recommended that administrators test any changes they plan to make prior to implementing them in production. If concerns arise about making changes to active volumes, engage technical support for assistance.

1. From the Access Policies tab under Group Configuration, create a new access policy or access policy group that reflects the access control needs of the volume.
2. Assign the new access policy to the volume. This can be done from either the targets pane on the access policies tab, or on the individual volume Access tab.
3. From the individual volume Access tab, delete the legacy basic access point.

This completes the process for changing the Access Control Policy.

**Note:** ISCSI connections that are logged into the volume under the old Basic Access Points access controls will persist until that connection is closed. A connection will be closed because the initiator no longer needs access to the volume, the OS is rebooted, or the connection is moved by the PS Group network load balancer to a different Ethernet port on the PS Group. For this reason, it may not become immediately apparent that a newly applied access control policy is not functioning in the manner intended by the administrator. Dell strongly recommends that any planned changes are verified prior to making the changes active in the production environment.

3.6 Copying access controls from another volume

This section explains how to copy the iSCSI access setting from an existing volume to a new volume. In this example, the volume name is CopyExample.

1. From the Volumes section, click Create volume. Provide a Name for the new volume, and then click Next to continue.
2. Set an appropriate size for the volume and click Next to continue.
3. In the Define iSCSI access point dialog box, select Copy access controls from another volume and then select the source volume. In this example, access controls are copied from the volume labeled FileServer.
4. Click Next to continue.
5. Select the appropriate Sector Size for the volume. See the firmware’s Group Administration guide for more information on the sector size feature. Click Next to continue.
6. The Summary page lists the options chosen when creating the volume, including the source volume for the access controls.

**Note:** It is important to remember that the access controls on the new volume are a copy, and are not linked back to the access controls on the original volume. Since the original volume used basic access points, changes to the access controls on the original volume do not impact the access controls on the new volume. If the copied access control was an access policy or access policy group, then the changes to the policy would be reflected on all of the volumes that inherit that policy.
4 Limits

An access record is either an extended access point or a basic access point. Compared to using basic access points, access control policies increase the number of access records that can be associated with an individual volume. Previously, an individual volume was limited to sixteen basic access points, and depending on the usage of IQNs or IP addresses, this could limit the number of servers in a cluster that could attach to an individual volume.

Access control policies have introduced a large degree of flexibility and increased scalability. Each volume can have a combined total of four access policies or access policy groups associated with it. Each access policy group, of which 128 can be defined within the PS Group, can contain up to 64 access policies. Each access policy can contain up to 16 extended access points. However, the group limits listed in Table 1 must be kept in mind when designing policies and groups.

It is possible to use both basic access points and access control policies on an individual volume. This is done when migrating a configured environment from using basic access points to using access control policies. While using both access control methods simultaneously is supported, it is important that all storage administrators of the environment are aware of the method used for particular volumes.

When combining access control policies and basic access points within the same PS Group, the access control policy limits may be lower depending on the total number of basic access points, as noted in the table below.

Table 1 Access policy limits

<table>
<thead>
<tr>
<th>Total basic access points</th>
<th>1023</th>
<th>2047</th>
<th>3071</th>
<th>3072+</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access policy groups</td>
<td>128</td>
<td>64</td>
<td>32</td>
<td>16</td>
</tr>
<tr>
<td>Access policies</td>
<td>512</td>
<td>256</td>
<td>128</td>
<td>64</td>
</tr>
<tr>
<td>Total extended access points</td>
<td>1024</td>
<td>512</td>
<td>256</td>
<td>128</td>
</tr>
<tr>
<td>Total extended access points if using IP addresses</td>
<td>2048</td>
<td>1024</td>
<td>512</td>
<td>256</td>
</tr>
<tr>
<td>Access policy associations</td>
<td>4096</td>
<td>2048</td>
<td>1024</td>
<td>512</td>
</tr>
</tbody>
</table>
5 Host Integration Toolkit compatibility

Dell EqualLogic provides Host Integration Toolkits for Microsoft Windows, VMware vSphere and Linux. It may be necessary to upgrade to a recent version of the toolkit being used prior to migration from the current volume access controls to using access control policies. Refer to the toolkit documentation for details on compatibility.
Glossary

Access control policies introduce some new terminology. For a full list of all EqualLogic storage technology terminology, see the *EqualLogic Master Glossary* included with each firmware release and available from the Dell EqualLogic Support website at eqlsupport.dell.com.

**Access control list (ACL):** A list of permissions assigned to a volume. See access policy, access policy group, and basic access point.

**Access control record:** As of PS Series firmware version 7.0, referred to as a *basic access point*.

**Access policy:** A set of extended access points that provide a method for describing endpoints for a volume. After an access policy is associated with a volume, all the endpoints described by the extended access points have access to that volume.

**Access policy group:** A set of access policies that can be assigned to a volume. All endpoints described within those access policies have access to that volume.

**Basic access point:** A traditional direct method for connecting a single endpoint to a single volume. Prior to PS Series firmware version 7.0, referred to as an *access control record*.