Role Based Access Controls (RBAC) Technical Overview & Enhancements

For Unisphere for PowerMax & Solutions Enabler 9.0

Dell Engineering
May 2018

ABSTRACT

Unisphere for PowerMax and Solutions Enabler 9.0 significantly changes the traditional behavior of Role Based Access Controls (RBAC/User Authorization) to better support local and remote replication environments. This document is intended for IT professionals who need to understand these RBAC enhancements to Unisphere for PowerMax and Solutions Enabler 9.0. It is specifically targeted at Dell EMC customers and field technical staff who are either running RBAC today or are considering RBAC as a viable user or array based security solution for their VMAX or PowerMax environments.
Revisions

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2018</td>
<td>Initial release</td>
</tr>
</tbody>
</table>

The information in this publication is provided “as is.” Dell Inc. makes no representations or warranties of any kind with respect to the information in this publication, and specifically disclaims implied warranties of merchantability or fitness for a particular purpose.

Use, copying, and distribution of any software described in this publication requires an applicable software license.

Copyright © April 2018 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA [4/20/2018] [Technical Overview] [H17132]

Dell believes the information in this document is accurate as of its publication date. The information is subject to change without notice.
# Table of contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revisions</td>
<td>2</td>
</tr>
<tr>
<td>Executive Summary</td>
<td>4</td>
</tr>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Enhancement Overview</td>
<td>6</td>
</tr>
<tr>
<td>Increased granularity for RBAC roles and resources</td>
<td>6</td>
</tr>
<tr>
<td>Enhancements to provide Storage Group wildcards</td>
<td>9</td>
</tr>
<tr>
<td>RBAC User-to-Role map visibility changes</td>
<td>10</td>
</tr>
<tr>
<td>Visibility to roles and access rights required</td>
<td>11</td>
</tr>
<tr>
<td>Updated Solutions Enabler and Unisphere Interfaces</td>
<td>12</td>
</tr>
<tr>
<td>Detailed functionality by role</td>
<td>15</td>
</tr>
<tr>
<td>Summary</td>
<td>18</td>
</tr>
</tbody>
</table>
Executive Summary

The Role Based Access Control (RBAC) or User Authorization (UserAuth) feature of Solutions Enabler provides a method for restricting the management operations that individual users or groups of users may perform on VMAX, VMAX AF, and PowerMax family arrays. Symmetrix Access Controls (SymACL), in contrast, is a feature of the HYPERMAX OS or PowerMax OS environments that allows an administrator to restrict host access to defined sets of devices (access pools) or granular features in a VMAX family array for security or segregation of management purposes.

RBAC enhancements with Unisphere for PowerMax and Solutions Enabler 9.0 or later implement many features already present in the SymACL implementation, making RBAC a viable alternative to SymACL for many to most customers. With Solutions Enabler 9.0, a number of enhancements have been made to the RBAC feature. These include:

- Increased granularity for RBAC roles and resources
- RBAC User-to-Role map visibility changes
- Visibility to roles and access rights required
- Enhancements to provide Storage Group wildcards

These enhancements provide the following direct benefits to the user:

- Provides a more granular support by providing users with rights to operate on individual applications (via Storage Groups or SGs) to application administrators, but not the entire array (ex. Ability to target Basic SGs or Parent SG of a cascaded group)
- Provides the administrator with the ability to further target user access to a specific replication role, distinct access for local and remote replication features
- REST API integration allowing associated scripts to take advantage of these RBAC controls to simplify the management stack and overall maintenance as well as eliminate the need to deploy Solutions Enabler Gatekeeper devices

AUDIENCE

This document is intended for IT professionals who need to understand these RBAC enhancements to Unisphere for PowerMax and Solutions Enabler 9.0. It is specifically targeted at Dell EMC customers and field technical staff who are either running RBAC today or are considering RBAC as a viable user or array based security solution for their VMAX or PowerMax environments.
Introduction

RBAC is managed using Unisphere for VMAX, Unisphere for PowerMax, or the Solutions Enabler CLI symauth command. Using symauth, a user or group of users, may be mapped to a specific access role, which defines the operations that these users are permitted to perform on the entire VMAX array.

There are currently 7 user defined roles that are available with RBAC: None, Monitor, PerfMonitor, StorageAdmin, SecurityAdmin, Admin, and Auditor. Listed below are the base capabilities of these current roles:

- **None**  No capabilities
- **Monitor**  Performs read-only operations on an array excluding the ability to read the audit log or Access Control definitions.
- **PerfMonitor**  Includes Monitor role permissions and grants additional privileges within the performance component of Unisphere for VMAX application to set up various alerts and update thresholds to monitor array performance.
- **StorageAdmin**  Perform all management and control functions. Please see specific section pertaining to this role below.
- **SecurityAdmin**  Performs security operations (symaudit , symacl , symauth ) on an array in addition to all monitor operations. Users or groups assigned the SecurityAdmin or Admin roles can create or delete component-specific authorization rules. The SecurityAdmin also has all Auditor rights.
- **Admin**  Performs all operations on an array, including security operations and monitor operations. The Admin also has storageAdmin rights, SecurityAdmin rights, and application performance monitoring privileges.
- **Auditor**  Grants the ability to view, but not modify, security settings for an array (including reading the audit log, symacl list , and symauth ) in addition to all monitor operations. This is the minimum role required to view the array audit log.

**UNDERSTANDING THE EXISTING STORAGEADMIN ROLE**

The StorageAdmin role, specifically, performs all management operations on an array or on individual components within an array in addition to all monitor operations. StorageAdmin was the only role that could be given access rights to modify the most commonly used features within an array and was therefore the predominant role provided to VMAX storage administrators.

Prior to Solutions Enabler 9.0, feature and device granularity continued to be limited regarding the ability to further subdivide access to individual device pools and target specific advanced features such as local and remote replication.

As part of these enhancements, the existing StorageAdmin role will remain the same; however, there will be a number of new roles defined that provide a subset of the rights held by the existing StorageAdmin role. It will also be possible to target each of these new roles to one or more Storage Groups (applications), allowing operation on only those groups and the devices that they contain.

Only these new roles will be able to target individual Storage Groups while all existing roles such as StorageAdmin will continue to be limited to the entire array.
Enhancement Overview

With Solutions Enabler 9.0, a number of enhancements have been made to the RBAC feature. These features include the following which will further expanded upon in dedicated sections below:

- Increased granularity to RBAC roles and resources
- Enhancements to provide Storage Group wildcards
- RBAC User-to-Role map visibility changes
- Visibility to roles and access rights needed for an operation

As part of these enhancements, there will be a number of new roles defined that provide a subset of the rights held by the existing StorageAdmin role. It is important to understand that these features are not based on the code version of the array and are therefore applicable to earlier storage systems which support Solution Enabler 9.0 and later.

Increased granularity for RBAC roles and resources

As noted above, the existing StorageAdmin role described above will remain; however, there will be three new roles available which will each comprise a subset of the overall StorageAdmin role responsibilities. These new sub-roles will be the following to include the area of responsibility:

- **LocalRep** New role encompassing local replication rights
- **RemoteRep** New role encompassing remote replication rights
- **DeviceManage** New role encompassing device management

It is possible to assign one of these sub-roles to users for one or more Storage Groups, allowing operation on only those Groups and the devices that they contain. Users can also be assigned a given role for devices visible to the host they are operating from, allowing operations allowed by the role to be carried out on only those devices.

The relationship of these new sub-roles to existing roles is as follows with a more detailed description of these roles below:
NEW LOCALREP ROLE
The operations allowed or restricted when a user is assigned the new LocalRep role are the following:

- Create, operate upon or delete SnapVX snapshots
- For SnapVX Restore operations, both LocalRep and DeviceManage roles are needed on the source devices
- For Link, Unlink, Relink, Set Copy and Set NoCopy SnapVX operations, DeviceManage rights are needed on the linked devices, while LocalRep role is needed on the source devices
- **Not allowed:** Creation of Secure SnapVX snapshots. For that, the greater StorageAdmin role is needed

This role automatically grants MONITOR rights and may be assigned at the Storage Group level.

NEW REMOTE REP ROLE
The operations allowed or restricted when a user is assigned the new RemoteRep role are the following:

- Create, operate upon or delete SRDF device pairs
- Set non-SRDF/A related attributes on an SRDF group – but only if the RBAC RemoteRep role is applied to the entire VMAX array

**Not Allowed:**

- Create or delete SRDF groups
- Modification of SRDF/A SRDF group attributes. The setting of SRDF/A SRDF group attributes requires StorageAdmin role

This role automatically grants MONITOR rights and may be assigned at the Storage Group level.

NEW DEVICEMANAGE ROLE
The operations allowed or restricted when a user is assigned the new DeviceManage role are the following:

- Perform control operations (Ready, not-Ready, Free, etc.) on devices
- Perform configuration operations (set names, flags, etc.) on devices
- Obtain or release Device Locks on devices
- Perform Link, Unlink, Relink, Set Copy and Set NoCopy operations on SnapVX link devices
- If LocalRep rights are also present, perform Restore operations to SnapVX source devices

**Not allowed:** The creation, expansion or deletion of devices. For those, the greater StorageAdmin role is needed

This role automatically grants MONITOR rights and may be assigned at the Storage Group level.

REVISITING THE STORAGEADMIN ROLE
Based on the new roles of LocalRep, RemoteRep, and DeviceManage described above, it is important to revisit the operations that will continue to be accomplished via the existing StorageAdmin role in context of these new enhancements:

- Perform array configuration operations
- Provision or delete storage
- Create, modify or delete masking objects: SGs, IGs, PGs, MVs
• Any operations granted by the LocalRep, RemoteRep, DeviceManage roles

• **The creation of Secure SnapVX snapshots**

This role automatically grants LocalRep, RemoteRep, DeviceManage, and Monitor roles and must be assigned to the entire array rather than the Storage Group level as is the case with the new roles described above.
Enhancements to provide Storage Group wildcards

As noted previously, the new roles of LocalRep, RemoteRep, and DeviceManage may be granted to one or more Storage Groups. A feature provided by both Unisphere for PowerMax and Solutions Enabler 9.0 or later allows a single Storage Group definition to cover multiple groups via a wildcard matching facility.

When assigning a Storage Group with these new roles, the following wildcards may be utilized:

- **abc**  
  Exactly these characters

- **?**  
  Any 1 character

- **+**  
  Any zero or more characters

- **[]**  
  Zero or more additional occurrences of the previous match

- **[a-zA-Z]**  
  Any of these characters

- **[!a-zA-Z]**  
  Anything but one of these characters

The following examples show how these wildcard patterns will be interpreted:

<table>
<thead>
<tr>
<th>This pattern</th>
<th>Matches these SGs</th>
<th>But not these</th>
</tr>
</thead>
<tbody>
<tr>
<td>tg_*</td>
<td>tg_DB_SG1</td>
<td>tgNewSG</td>
</tr>
<tr>
<td></td>
<td>tg_newSG</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TG_sg_db</td>
<td></td>
</tr>
<tr>
<td>prod_sg?</td>
<td>prod_sg1</td>
<td>prod_sg12</td>
</tr>
<tr>
<td></td>
<td>prod_sga</td>
<td>prod_sgab</td>
</tr>
<tr>
<td></td>
<td>Prod_sg2</td>
<td></td>
</tr>
<tr>
<td>prod_sg[0-9]+</td>
<td>prod_sg1</td>
<td>prod_sga</td>
</tr>
<tr>
<td></td>
<td>prod_sg12</td>
<td>prod_sgab</td>
</tr>
</tbody>
</table>

The only allowed characters are: a-zA-Z0-9_ along with the above *+?[]! wildcard characters. As noted previously, the only roles that can be assigned against Storage Groups are: Local Rep, Remote Rep and Device Manage. Storage Groups do not have to exist at the time that a matching RBAC rule for them is defined.

These Storage Group level RBAC rules are only applicable to parent and stand-alone Storage Groups and not child Storage Groups. Child Storage Groups are protected by the RBAC rules, if any, on their parent Storage Group.
RBAC User-to-Role map visibility changes

Currently, users may view the full set of RBAC roles defined per array. Solutions Enabler 9.0 now allows a security administrator to change this default behavior via a new Secure Reads policy. If this new policy is enabled, only users assigned to a role of Admin, SecurityAdmin or Auditor will be able to view all defined RBAC roles.

All other users will only be able to view RBAC roles that either (a) apply to them or (b) assigned a role of Admin or SecurityAdmin. If disabled, all users will be able to view all defined RBAC rules, preserving the existing default behavior.

To set/unset the Secure Reads policy, the following command is used:

    symauth -sid xxx set secure_reads enable | disable

To view if this policy is in effort, the following command is used:

    symauth -sid xxx list

      SYMMETRIX AUTHORIZATION STATUS

Symmetrix ID: 000196801476

  Authorization Control : Disabled

  Time Enabled          : N/A
  Time Disabled         : N/A
  Time Updated          : N/A

  Enforcement Mode      : Enforce
  Secure Reads          : Disabled
Visibility to roles and access rights required

Currently, there is no convenient way for a customer to determine the Symmetrix Access Control (SymACL) access rights or RBAC role needed to perform certain operations. This can make it difficult to determine to configure the required access rights (in the case of SymACL) or RBAC roles required to successfully allow the desired operation.

A mechanism has been implemented in Solutions Enabler 9.0 to allow a user to run in a mode where the individual SymACL access rights and RBAC roles are reported to the host SYMAPI Log as Solutions Enabler checks for them. A new environment variable, SYMAPI_LOG_ACCESS_CHECKS, has been created to control this reporting behavior.

To set the SYMAPI_LOG_ACCESS_CHECKS environment variable:

Unix
```bash
export SYMAPI_LOG_ACCESS_CHECKS = TRUE
```

Windows
```sql
set SYMAPI_LOG_ACCESS_CHECKS = TRUE
```

The following are SYMAPI Log examples noting the reported requirements for SymACL access rights and RBAC roles:

**SymACL access type:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>PID</th>
<th>User</th>
<th>Process</th>
<th>Access Type</th>
<th>SYMAPI Log Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/28/2017</td>
<td>14:28:40</td>
<td>23799</td>
<td>EMC:Internal_Test</td>
<td>SymSnapVXControl</td>
<td>SNAP</td>
<td>Checking for ACL</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SID 000197800188</td>
<td></td>
</tr>
</tbody>
</table>

**RBAC Role:**

<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>PID</th>
<th>User</th>
<th>Process</th>
<th>Roles</th>
<th>SYMAPI Log Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/28/2017</td>
<td>14:31:01</td>
<td>23871</td>
<td>EMC:Internal_Test</td>
<td>SymSnapVXControl</td>
<td>LocalRep [StorGrp=test1]</td>
<td>Checking for RBAC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SID 000197800188</td>
<td></td>
</tr>
</tbody>
</table>

Note: Only the minimum set of roles/rights will be logged for RBAC.
Updated Solutions Enabler and Unisphere Interfaces

This section provides and examples of the changes made to both the Unisphere for PowerMax and Solutions Enabler 9.0 SYMCLI interfaces to support the enhancement describes in this document.

**Solutions Enabler SYMCLI**

The following SYMCLI example assigns a user with the new RBAC roles with wildcard Storage Group definitions:

```bash
symauth -sid 1476 commit
assign user H:dldv0182\tgamdm to role LocalRep+DeviceManage for StorGrp tg_*;
assign user H:dldv0182\tgamdm to role DeviceManage for StorGrp host1_*;
```

The following SYMCLI example provides a view of the User-to-Role map assigning users with the new RBAC roles with wildcard Storage Group definitions:

```
symauth -sid 476 list -users -by_user
```

**SYMEXTRIX AUTHORIZATION USERS**

Symmetrix ID: 000196801476

<table>
<thead>
<tr>
<th>User/Group name</th>
<th>Role</th>
<th>Component</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>User H:dldv0182\russo</td>
<td>LocalRep</td>
<td>N/A</td>
<td></td>
</tr>
<tr>
<td>User H:dldv0182\russo</td>
<td>PerfMonitor</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User H:dlqv0182\tgamdm</td>
<td>LocalRep</td>
<td>StorGrp:tg_*</td>
<td></td>
</tr>
<tr>
<td>User H:dlqv0182\tgamdm</td>
<td>DeviceManage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>User H:dlqv0182\tgamdm</td>
<td>LocalRep</td>
<td>StorGrp:host1_*</td>
<td></td>
</tr>
</tbody>
</table>
Unisphere for PowerMax

The following Unisphere for PowerMax example assigns a new user with the new RBAC roles with wildcard Storage Group definitions:
Role Based Access Controls (RBAC) Technical Overview & Enhancements
Detailed functionality by role

This section describes the capability and dependencies provided by all current and new RBAC roles:

**Existing Monitor Role**
The operations allowed or restricted when a user is assigned the existing Monitor role are the following:

- Role allows a user to perform passive (show, list, view) operations:
  - View array information
  - View masking object information (SGs, IGs, PGs, MVs)
  - View device information
- **Not Allowed:** The viewing of security related data: Symmetrix ACL DB, RBAC User-to-Role Map, and the Symmetrix Audit Log

**Existing Performance Monitor Role**
The operations allowed or restricted when a user is assigned the existing Monitor role are the following:

- This role is only utilized by Unisphere
- This role allows a user to configure Unisphere performance alerts and thresholds

This role automatically grants MONITOR rights and must be assigned to the entire array rather than the Storage Group level.

**Existing Auditor Role**
The operations allowed or restricted when a user is assigned the existing Monitor role are the following:

- View Symmetrix ACL Database
- View RBAC User-to-Role Map and settings
- View the Symmetrix Audit log

This role automatically grants MONITOR rights and must be assigned to the entire array rather than the Storage Group level.

**Existing SecurityAdmin Role**
The operations allowed or restricted when a user is assigned the existing SecurityAdmin role are the following:

- Modify Symmetrix ACL Database
- Modify RBAC User-to-Role Map and settings

This role automatically grants MONITOR rights and must be assigned to the entire array rather than the Storage Group level.
New LocalRep Role
The operations allowed or restricted when a user is assigned the new LocalRep role are the following:

- Create, operate upon or delete SnapVX snapshots
- For SnapVX Restore operations, both LocalRep and DeviceManage roles are needed on the source devices
- For Link, Unlink, Relink, Set Copy and Set NoCopy SnapVX operations, DeviceManage rights are needed on the linked devices, while LocalRep role is needed on the source devices
- Not allowed: Creation of Secure SnapVX snapshots. For that, the greater StorageAdmin role is needed

This role automatically grants MONITOR rights and may be assigned at the Storage Group level.

New RemoteRep Role
The operations allowed or restricted when a user is assigned the new RemoteRep role are the following:

- Create, operate upon or delete SRDF device pairs
- Set non-SRDF/A related attributes on an SRDF group – but only if the RBAC RemoteRep role is applied to the entire VMAX array

Not Allowed:

- Create or delete SRDF groups
- Modification of SRDF/A SRDF group attributes. The setting of SRDF/A SRDF group attributes requires StorageAdmin role

This role automatically grants MONITOR rights and may be assigned at the Storage Group level.

New DeviceManage Role
The operations allowed or restricted when a user is assigned the new DeviceManage role are the following:

- Perform control operations (Ready, not-Ready, Free, etc.) on devices
- Perform configuration operations (set names, flags, etc.) on devices
- Obtain or release Device Locks on devices
- Perform Link, Unlink, Relink, Set Copy and Set NoCopy operations on SnapVX link devices
- If LocalRep rights are also present, perform Restore operations to SnapVX source devices
- Not allowed: The creation, expansion or deletion of devices. For those, the greater StorageAdmin role is needed

This role automatically grants MONITOR rights and may be assigned at the Storage Group level.
**Existing StorageAdmin Role**

The operations allowed or restricted when a user is assigned the existing StorageAdmin role are the following:

- Perform array configuration operations
- Provision or delete storage
- Create, modify or delete masking objects: SGs, IGs, PGs, MVs
- Any operations granted by the LocalRep, RemoteRep, DeviceManage roles
- **The creation of Secure SnapVX snapshots**

This role automatically grants LocalRep, RemoteRep, DeviceManage, and Monitor roles and must be assigned to the entire array rather than the Storage Group level as is the case with the new roles described above.

**Existing Admin Role**

The operations allowed or restricted when a user is assigned the existing Admin role are the following:

- This role allows a user to perform all operations
- Grants a combination of StorageAdmin and SecurityAdmin roles
Summary

The Role Based Access Control (RBAC) or User Authorization (UserAuth) feature of Solutions Enabler provides a method for restricting the management operations that individual users or groups of users may perform on VMAX, VMAX AF, and PowerMax family arrays. Symmetrix Access Controls (SymACL), in contrast, is a feature of the HYPERMAX OS or PowerMax OS environments that allows an administrator to restrict host access to defined sets of devices (access pools) or granular features in a VMAX family array for security or segregation of management purposes.

RBAC enhancements with Solutions Enabler 9.0 or greater implement many features already present in the SymACL implementation, making RBAC a viable alternative to SymACL for many to most customers. With Solutions Enabler 9.0, a number of enhancements have been made to the RBAC feature. These include:

- Increased granularity to RBAC roles and resources
- RBAC User-to-Role map visibility changes
- Visibility to roles and access rights required
- Enhancements to provide Storage Group wildcards

These enhancements provide the following direct benefits to the user:

- Provides a more granular support by providing users with rights to operate on individual applications (via Storage Groups or SGs) to application administrators, but not the entire array (ex. Ability to target Basic SGs or Parent SG of a cascaded group)
- Provides the administrator with the ability to further target user access to a specific replication role, distinct access for local and remote
- REST API integration allowing associated scripts to take advantage of these RBAC controls to simplify the management stack and overall maintenance as well as eliminate the need to deploy Solutions Enabler Gatekeeper devices

With these enhancements, there will be three new roles available which will each comprise a subset of the overall StorageAdmin role responsibilities. These new sub-roles will be the following to include the area of responsibility:

- **LocalRep** New role encompassing local replication rights
- **RemoteRep** New role encompassing remote replication rights
- **DeviceManage** New role encompassing device management

It is possible to assign on of these sub-roles to users for one or more Storage Groups, allowing operation on only those Groups and the devices that they contain. Users can also be assigned a given role for devices visible to the host they are operating from, allowing operations allowed by the role to be carried out on only those devices.

These new roles may be granted to one or more Storage Groups. A feature provided by both Unisphere for PowerMax and Solutions Enabler 9.0 or later allows a single Storage Group definition to cover multiple groups via a wildcard matching facility.

Currently, users may view the full set of RBAC roles defined per array. Solutions Enabler 9.0 now allows a security administrator to change this default behavior via a new Secure Reads policy. If this new policy is enabled, only users assigned to a role of Admin, SecurityAdmin or Auditor will be able to view all defined RBAC roles.

A mechanism has been implemented in Solutions Enabler 9.0 to allow a user to run in a mode where the individual SymACL access rights and RBAC roles are reported to the host SYMAPI Log as Solutions Enabler checks for them. A new environment variable, `SYM_API_LOG_ACCESS_CHECKS`, has been created to control this reporting behavior.