Technical Report

# SnapDrive for Windows 6.2 in a Least Privilege Environment

Ron Demery, Allan Watanabe, NetApp
June 2010 | TR-3864

## SNAPDRIVE FOR WINDOWS STORAGE SYSTEM SERVICE ACCOUNT CAPABILITIES

This report was developed for administrators who require the NetApp® SnapDrive® for Windows® storage system service account to have minimal capabilities to perform its function.

TABLE OF CONTENTS

# 1 INTRODUCTION

Many IT environments today have policies that require the application service account to possess a minimal set of permissions. This is also driven by several standards that indicate the default accounts should be disabled because they are “well-known accounts.” NetApp recommends that in the NetApp Data ONTAP® operating system, the root account should be disabled.

Data ONTAP has the ability to configure a custom role and assign that role *permissions,* also known as *capabilities* in Data ONTAP. Refer to TR-3358: Role-Based Access Control for Data ONTAP 7G for the default roles and a fuller discussion of this topic.

"Security and Access Control" in TR-3828: Best Practices Guide for SnapDrive for Windows 6.2 discusses the use of various connection methods. This paper also contains information about the integration of SnapDrive for Windows (SDW) with Operations Manager RBAC and the use of the Storacl tool.

This report focuses on three levels of restrictions for the implementation of the SDW storage system service account: admin role, non-admin role, and least privilege role.

For information about the API calls to the Data ONTAP operating system, see the Manage ONTAP SDK.

# 2 THREE LEVELS OF RESTRICTIONS

The three levels of restrictions discussed in this document are admin role, non-admin role, and least privilege role.

### TEST ENVIRONMENT

Our test environment consisted of a Windows host with SnapDrive for Windows 6.2 and a NetApp storage system with Data ONTAP 7.3.1.1.

- Our connection to the storage system was through iSCSI without using CHAP for Authentication.
- NetApp SnapMirror® was licensed on the storage system.
- Administrative connection was initiated over HTTPS not using RPC or passthrough.

## 2.1 ADMIN ROLE

The admin role in the Data ONTAP operating system is the role with the most default permissions. An account with this role can control the configuration of the NetApp storage system in all aspects. This includes adding local storage system users, setting security values, and modifying the configuration options of the storage system. The admin role is by default associated with the storage system's Administrators group.

According to the SnapDrive 6.2 for Windows Installation and Administration Guide, NetApp recommends that the storage service account should be a member of the Data ONTAP Administrators group.

**Table 1) Default capabilities associated with the admin role.**

| Capability | Description |
|---|---|
| api-* | Grants the specified role the capability to execute all Data ONTAP API calls. |
| cli-* | Grants the specified role the capability to execute all CLI commands. |
| login-* | Grants the specified role telnet, console, rsh, ssh, and http-admin login capabilities. |
| security-* | Grants the specified role security-related capabilities, such as the ability to change other users’ passwords or to invoke the CLI priv set advanced command. |

## 2.2 NON-ADMIN ROLE

If you do not want to maintain the SnapDrive for Windows service account with the elevated permission set, follow the recommendations in the SnapDrive Windows Service Account capabilities thread on the NetApp Communities news board. This thread discusses how to create a role with the capabilities described in Table 2.

**Table 2) Non-admin role capabilities.**

| Capability | Description |
|---|---|
| api-aggr-* | These APIs allow full manipulation of Data ONTAP aggregates, including those embedded in traditional volumes and their structural components (plexes and RAID groups). |
| api-ems-* | The Event Management System (EMS) is a mechanism in the Data ONTAP kernel that supports creation, forwarding, and consumption of event indications. EMS events are generated by Data ONTAP when errors occur or to log changes in the status of the system. These event indications are logged to /etc/log/ems and, depending on the event and its severity, to the syslog console. If an event has an SNMP definition, SNMP traps are also generated by the event indication. |
| api-fcp-adapter-* | Read and write permissions to all API-initiated FCP-adapter operations: configuration, reset, and up and down status. |
| api-igroup-* | Read and write permissions to all API-initiated igroup operations: add bind, create, destroy, remove, rename, etc. |
| api-iscsi-* | Read and write permissions to all API-initiated iSCSI operations: service start and service stop, disable, destroy, create, enable, etc. |
| api-license-* | Read and write permissions to all API-initiated license operations: add, delete, and list. |
| api-lun-* | Read and write permissions to all API-initiated LUN operations: create, destroy, online, offline, etc. |
| api-qtree-* | Read and write permissions to all API-initiated qtree operations: create, destroy, list, rename, etc. |
| api-snapmirror-* | Read and write permissions to all API-initiated SnapMirror operations: service on, service off, break, abort, initialize, etc. |
| api-snapshot-* | Read and write permissions to all API-initiated Snapshot® operations: create, delete, rename, restore volume, restore volume, etc. |
| api-snapvault-* | Read and write permissions to all API-initiated SnapVault® operations: adding and removing relationships, schedule modifications, abort, create, restore, etc. |
| api-system-* | Read permissions to all API-initiated system operations: get version, get info, etc. |
| api-volume-* | Read and write permissions to all API-initiated volume operations: create, destroy, online offline, verify, split, restrict, size, etc. |
| login-* | Allows the account to log in via telnet, ssh, rsh, console, and http/s. |

This set of capabilities does not allow the service account to add local accounts to the storage system. This role must be created and then added to a new group. The service account can then be added to the new group. The role can be created via the command line or through Operations Manager.

### NON-ADMIN ROLE CREATION (COMMAND LINE METHOD)

```
toaster>useradmin role add SD-non-admin  -a login-*,api-lun-*,api-snapshot-
*,api-iscsi-*,api-volume-*,api-snapmirror-*,api-snapvault-*,api-ems-*,api-
igroup-*,api-qtree-*,api-fcp-adapter-*,api-license-*,api-system-*,api-aggr-*
```

## 2.3 LEAST PRIVILEGE ROLE

In some IT environments, a detailed assignment of the minimal permissions is required. Table 3 describes the capabilities that were needed to connect to the storage system from the SnapDrive for Windows 6.2 GUI by using a local account on the storage system. This local Data ONTAP account was assigned a customized role, which contained the capabilities.

**Table 3) Least privilege role capabilities to connect to the storage system with iSCSI LUNs.**

| Capability | Description from SDK – ONTAPI version 1.11 |
|---|---|
| api-aggr-list-info | Get aggregate status. |
| api-file-list-directory-iter-* | Obtain a list of files in a given directory. This includes the start, next, and end commands to develop the list. |
| api-igroup-list-info | Get information for initiator groups. |
| api-iscsi-adapter-list-info | Get the list of initiators currently connected to any of the portal groups associated with specified adapter. |
| api-iscsi-node-get-name | Return the current iSCSI node name. |
| api-iscsi-service-status | Get status of the iSCSI service, whether or not it is running. |
| api-license-list-info | Return information about the current list of licensed Data ONTAP services, their codes, the type of license, and, if it is a time-limited license, the expiration date. Also tells the services that are not licensed for your appliance, and if a time-limited licensed service has expired. |
| api-lun-clone-status-list-info | Get the cloning status of a LUN or LUNs. |
| api-lun-get-attribute | Get a named attribute for a given LUN. |
| api-lun-get-comment | Get the optional descriptive comment for a LUN. |
| api-lun-get-serial-number | Get the serial number for the specified LUN. |
| api-lun-get-space-reservation-info | Query the space reservation settings for the named LUN. |
| api-lun-has-scsi-reservations | Query for all types of SCSI reservations covering both iSCSI and FCP. |
| api-lun-initiator-logged-in | Determine whether an initiator is logged in via FCP or iSCSI. |
| api-lun-list-info | Get the status (size, online/offline state, shared state, comment string, serial number, LUN mapping) of the given LUN or of all LUNs. |
| api-lun-map | Map the LUN to all the initiators in the specified initiator group. |
| api-lun-map-list-info | Return a list of initiator groups and their members (the initiators) mapped to the given LUN. |
| api-lun-online | Reenable block-protocol accesses to the LUN. |
| api-lun-read-raw | Read a LUN |
| api-lun-set-attribute | Set a named attribute for a given LUN. |
| api-lun-set-comment | Set the optional descriptive comment for a LUN. |
| api-lun-set-space-reservation-info | Set the space reservation settings for the named LUN. |
| api-lun-unmap | Reverse the effect of lun-map on the specified LUN for the specified group. |
| api-lun-write-raw | Write to a LUN |

| Capability | Description from SDK – ONTAPI version 1.11 |
|---|---|
| api-qtree-list | Return a list of qtrees. |
| api-snapmirror-get-status | Return the SnapMirror status. |
| api-snapshot-get-schedule | Obtain the current Snapshot schedule on a specified volume. |
| api-snapshot-set-schedule | Set the Snapshot schedule on a specified volume. |
| api-snapvault-primary-get-relationship-status | Request the primary to return the status entries for the desired relationships. |
| api-system-get-info | Obtain appliance information, including CPU and backplane information. |
| api-system-get-version | Obtain the Data ONTAP version. |
| api-volume-clone-create | Create a flexible volume that is a clone of a "backing" or "parent" flexible volume. |
| api-volume-container | Return the name of the containing aggregate for the named flexible volume. |
| api-volume-destroy | Destroy the specified volume or plex. |
| api-volume-get-root-name | Name of the root volume for the storage system. |
| api-volume-list-info | Return a list of volumes and their status information. |
| api-volume-offline | Take the specified volume or plex offline, making it unavailable for both user-level data access and RAID-level access (unless it's a flexible volume, in which case its containing aggregate is not affected in any way, and remains fully online). |
| api-volume-options-list-info | Get the options that have been set for the specified volume. |
| login-http-admin | Require the permission to log in via port 80 or 443. |

Once we achieved a connection to the storage system, we started exercising the GUI to perform various LUN operations. Table 4 describes the capabilities that we found **necessary to add to the role** in order to perform the function indicated. As an example: In order to create a LUN it would be necessary to have all the capabilities listed in table 3 as well as the api-lun-get-maxsize and the api-lun-create-by-size as listed in table 4.

**Table 4) Additional capabilities required for performing functions in SnapDrive for Windows after connection.**

| Capability | Description from SDK – ONTAPI version 1.11 | SDW Function |
|---|---|---|
| api-lun-get-maxsize | Returns the maximum possible size in bytes of a LUN on a given volume or qtree. | Create a LUN |
| api-lun-create-by-size | Create a new LUN of a given size, with initially zero contents. | Create a LUN |
| api-lun-initiator-list-map-info | List all LUNs that are mapped to an initiator. | Manage igroup settings |
| api-lun-destroy | Destroy the specified LUN. | Delete a LUN |
| api-snapshot-list-info | Return Snapshot information for a specified volume. | Create a Snapshot copy |
| api-snapshot-create | Create a new Snapshot copy on a specified volume. | Create a Snapshot copy |

| Capability | Description from SDK – ONTAPI version 1.11 | SDW Function |
|---|---|---|
| api-snapshot-delete | Delete a Snapshot copy from a specified volume. | Delete a Snapshot copy |
| api-ems-autosupport-log | Used by SnapDrive to log SnapDrive specific events occurring on a host system to the appliance and optionally to use the appliance to generate an AutoSupport message. | Delete a Snapshot copy |
| api-snapshot-restore-file | Revert a single file to a revision from a specified Snapshot copy. | Restore a Snapshot copy |
| api-options-get | Get the value of a single option. | Restore a Snapshot copy |
| api-snapshot-rename | Rename a specified Snapshot copy to a new name on a specified volume. | Rename a Snapshot copy |
| api-lun-resize | Change the size of the LUN. | Resize a LUN |
| api-lun-get-occupied-size | Get the size occupied by the LUN in the active file system. | Run Space Reclaimer |
| api-snapmirror-get-volume-status | Return SnapMirror status values for a given volume. | Use SnapMirror |
| api-snapmirror-list-destinations | Return a list of destination locations and information about SnapMirror relationships for given source locations, which can be a volume name or a qtree path. | Use SnapMirror |
| api-snapmirror-update | Start a transfer over the network for a specific destination. | Use Snapmirror |

This set of capabilities does not allow the service account to add local accounts to the storage system. This role must be created and then added to a new group. The service account can then be added to the new group. The role can be created via the command line or through Operations Manager.

### LEAST PRIVILEGE ROLE CREATION (COMMAND LINE METHOD)

In developing this report, we discovered that it was necessary to create several roles because of the character limit of the text editor we used.

```
toaster> useradmin role add SD_leastPriv1 -a login-http-admin,api-system-get-
version,api-license-list-info,api-volume-list-info,api-volume-get-root-name,api-
volume-container,api-file-list-directory-iter-*,api-lun-clone-status-list-
info,api-lun-list-info
Sun May 18 15:08:29 EDT [toaster: useradmin.added.deleted:info]: The role
'SD_leastPriv1' has been added.
Role <SD_leastPriv1> added.

toaster> useradmin role add SD_leastPriv2 -a api-system-get-info,api-lun-get-
comment,api-lun-get-space-reservation-info,api-snapmirror-get-status,api-qtree-
list,api-lun-get-attribute,api-volume-options-list-info,api-snapvault-primary-
get-relationship-status,api-lun-has-scsi-reservations,api-lun-map-list-info,api-
snapshot-get-schedule
Sun May 18 15:09:41 EDT [toaster: useradmin.added.deleted:info]: The role
'SD_leastPriv2' has been added.
Role <SD_leastPriv2> added.
```

```
toaster> useradmin role add SD_leastPriv3 -a api-iscsi-service-status,api-iscsi-
node-get-name,api-iscsi-adapter-list-info,api-aggr-list-info,api-volume-clone-
create,api-lun-set-attribute,api-igroup-list-info,api-snapshot-set-schedule,api-
lun-write-raw,api-volume-offline,api-lun-set-space-reservation-info,api-volume-
destroy,api-lun-initiator-logged-in
Sun May 18 15:11:23 EDT [toaster: useradmin.added.deleted:info]: The role
'SD_leastPriv3' has been added.
Role <SD_leastPriv3> added.

toaster> useradmin role add SD_leastPriv4 -a api-lun-online,api-lun-read-
raw,api-lun-map,api-lun-unmap,api-lun-get-serial-number,api-lun-set-comment
Sun May 18 15:14:32 EDT [toaster: useradmin.added.deleted:info]: The role
'SD_leastPriv4' has been added.
Role <SD_leastPriv4> added.


toaster> useradmin role add SD_leastPriv5 -a api-lun-get-maxsize,api-lun-create-
by-size,api-lun-initiator-list-map-info,api-lun-destroy,api-snapshot-list-
info,api-snapshot-create,api-snapshot-delete,api-ems-autosupport-log,api-
snapshot-restore-file,api-options-get,api-snapshot-rename,api-lun-resize,api-
lun-get-occupied-size,api-snapmirror-get-volume-status,api-snapmirror-list-
destinations,api-snapmirror-update
Sun May 18 15:20:16 EDT [toaster: useradmin.added.deleted:info]: The role
'SD_leastPriv5' has been added.
Role <SD_leastPriv5> added.

toaster> useradmin group add SDAdmin -r
SD_leastPriv1,SD_leastPriv2,SD_leastPriv3,SD_leastPriv4,SD_leastPriv5
Sun May 18 15:22:35 EDT [toaster: useradmin.added.deleted:info]: The group
'SDAdmin' has been added.
Group <SDAdmin> added.

toaster> useradmin group list SDAdmin
Name: SDAdmin
Info:
Rid: 131073
Roles: SD_leastPriv1,SD_leastPriv2,SD_leastPriv3,SD_leastPriv4,SD_leastPriv5
Allowed Capabilities: login-http-admin,api-system-get-version,api-license-list-
info,api-volume-list-info,api-volume-get-root-name,api-volume-container,api-
file-list-directory-iter-*,api-lun-clone-status-list-info,api-lun-list-info,api-
system-get-info,api-lun-get-comment,api-lun-get-space-reservation-info,api-
snapmirror-get-status,api-qtree-list,api-lun-get-attribute,api-volume-options-
list-info,api-snapvault-primary-get-relationship-status,api-lun-has-scsi-
reservations,api-lun-map-list-info,api-snapshot-get-schedule,api-iscsi-service-
status,api-iscsi-node-get-name,api-iscsi-adapter-list-info,api-aggr-list-
info,api-volume-clone-create,api-lun-set-attribute,api-igroup-list-info,api-
snapshot-set-schedule,api-lun-write-raw,api-volume-offline,api-lun-set-space-
reservation-info,api-volume-destroy,api-lun-initiator-logged-in,api-lun-
online,api-lun-read-raw,api-lun-map,api-lun-unmap,api-lun-get-serial-number,api-
lun-set-comment,api-lun-get-maxsize,api-lun-create-by-size,api-lun-initiator-
list-map-info,api-lun-destroy,api-snapshot-list-info,api-snapshot-create,api-
snapshot-delete,api-ems-autosupport-log,api-snapshot-restore-file,api-options-
get,api-snapshot-rename,api-lun-resize,api-lun-get-occupied-size,api-snapmirror-
get-volume-status,api-snapmirror-list-destinations,api-snapmirror-update
```

# 3 CONCLUSION

Every IT environment has different security postures, and therefore it is necessary to understand the interactions of applications with the operating system. This is especially true for application service accounts. These accounts usually require an elevated privilege to operate. Care should be taken to protect the account name and credentials at all times, because these accounts are sometimes more powerful than the normal administrative accounts.



www.netapp.com