

Dell EMC PowerMax and VMAX All Flash: Data Protector for z Systems (zDP) Best Practices

Abstract

This document provides best practices for Dell EMC™ Data Protector for z Systems (zDP), a tool that automates data preservation and recovery.

September 2020

Revisions

Date	Description
September 2020	Initial release: PowerMaxOS Q3 2020

Acknowledgments

Author: Justin Bastin

Contributors: Mark Grinnell

Support: Dell EMC Storage Technical Marketing Engineering Team

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 © 2020 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, EMC, Dell EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners. [9/16/2020] [Best Practices] [H18472]

Table of contents

Revisions.....	2
Acknowledgments.....	2
Table of contents	3
Executive summary.....	4
Audience	4
1 Introduction.....	5
1.1 Terminology	5
2 Configuring zDP for ISPF	6
2.1 zDP ISPF best practices.....	6
2.2 zDP naming best practices.....	6
2.3 zDP definition best practices	6
2.4 zDP monitoring best practices.....	8
3 Space considerations	11
4 Deploying local-array SnapVX and zDP	12
5 Deploying remote-array TimeFinder SnapVX and zDP	13
6 Secure snapshots.....	14
7 Operational best practices.....	15
8 Summary	16
A Technical support and resources	17

Executive summary

Finding new and creative ways to preserve data in a digital age requires thorough planning before production implementation. Organizations must also consider the legal and financial ramifications by not providing safety for their data assets.

Since 2016, Dell EMC™ Data Protector for z Systems (zDP) has provided automated data preservation that enables organizations to restore their data in the event of logical corruption. zDP is built upon Dell EMC TimeFinder™ SnapVX and can create space-efficient snapshots using a fraction of the storage (based on data change rate).

Although environments may vary, this document provides suggestions and best practices for organizations to consider before, during, and after zDP implementation.

Audience

This document is intended for information technology professionals, z/OS systems architects, and IT storage administrators. This document assumes the reader has a basic knowledge of Dell EMC PowerMax and VMAX™ All Flash technologies. Readers should also review the document [Dell EMC PowerMax and VMAX All Flash: Data Protector for z Systems \(zDP\) Essentials](#) before reading this paper.

1 Introduction

Data Protector for z Systems (zDP) is a mainframe software solution that provides continuous data protection for your mainframe data assets. Deployed upon the Dell EMC TimeFinder SnapVX space-efficient volume-snap capability, your environment can increase the granularity of application recovery. zDP uses three main components to increase granularity: versioned data groups (VDG), snapsets, and target sets. To assist with zDP, the software can manage, operate, and monitor your environment through JCL and SCF commands. These components work together to provide seamless integration and enable your backups to use zDP.

1.1 Terminology

Data Protector for z Systems (zDP): Dell EMC software that provides granular data backups.

TimeFinder SnapVX: Backup technology that is built on virtual provisioning and enables you to take snapshots of Dell EMC source volumes on VMAX arrays.

Local snapshot: Data copy that is taken at the source PowerMax array.

Remote snapshot: Data copy that is taken at the target or remote PowerMax array.

Versioned data group (VDG): Logical group of source volumes that associates volumes and settings for creating multiple point-in-time images.

Snapshot: Pointer-based, point-in-time image of single volume.

Snapset: Named point-in-time consistent image of all source-volume snapshots in a VDG.

Snapset capture: Continuous automated process of creating snapsets.

Target set: Group of devices which have been defined to zDP as the specified link targets to a snapset.

Secure VDG: Secured snapset that cannot be deleted. You can delete a secure VDG snapset by either allowing the interval set from snapset creation to expire, or following an approved procedure with help from Dell Support.

2 Configuring zDP for ISPF

When configuring zDP, you must configure the zDP ISPF REXX by editing your EIPCLIST parmlib member in the Dell EMC Mainframe Enablers SAMPLIB dataset. Update the following fields:

- **DS_PREFIX:** Provide the HLQ.qualifier of your Mainframe Enablers datasets. For example, if your dataset for SAMPLIB is ICO.MFE8.SAMPLIB, the DS_PREFIX would be **ICO.MFE8**.
- **SCF_SUFFIX:** Provide this setting in the address-space-parameter library for the running EMCSCF instance. It is specified in the SCF.INI.CPFX setting.
- **SCF_JOBNAME:** This is the name of the running EMCSCF address space. To get the list of started tasks, perform the command **/D A,L** in **z/OS SYSLOG**.
- **UNIT:** Input the esoteric that is used in your environment for disk. Examples are SYSDA, 3390, SYSALLDA.
- **EIP_LOAD_LIBRARY:** This setting is the LOADLIB of your Mainframe Enablers software product.

2.1 zDP ISPF best practices

zDP delivers the ISPF panel in the HLQ.SAMPLIB > member EIPCLIST. After customizing EIPCLIST, run the REXX to configure, manage, and monitor the zDP environment through ISPF panels. Here are a few best practices for setting up and working with the zDP ISPF panels:

- After installing the mainframe enablers, copy the member into a new member, and update the copy EIPCLIST. This way preserves the original EIPCLIST that is delivered by Dell Technologies if you inadvertently mistype information when editing EIPCLIST.
- After starting zDP ISPF, you must update the **S Set Options** panel.
- In the S Set Options panel, note the **VDG Member Library** and **TGT Member Library** for future use. This dataset preserves all VDG or TGT definitions if you save them in the zDP ISPF panel
- Use the ISPF panel to create the VDG or TGT JCL control statements. After the ISPF preserves the JCL in the VDG or TGT Member Library, go to the respective library and copy the statements in your batch job. This ensures that you are using the most up-to-date parameters and defaults when creating your VDG and target groups.
- Use the zDP ISPF Help panels to raise awareness for the zDP components. In the zDP ISPF panels, press **F1** to access the help panels.

2.2 zDP naming best practices

Ensure that the volume data group and target names meet the naming standards of your environment. Ensure that the VDG is meaningful and represents the reason for the VDG. We do not recommend using timestamps in the name because each snapshot will have its own unique date and timestamp. You may also use the application name in the VDG name to represent which application exists in the VDG.

2.3 zDP definition best practices

zDP can take snapshots with a five-minute granularity at minimum. You must evaluate your data-retention needs to preserve data if there is a logical corruption. These deployment practices are suggestions to provide direction, and can help you consider the impacts of data retention and recoverability.

If your storage environment is sized correctly to 120 snapshots, the following implementation provides granularity and increased security with your zDP snapshots.

- Set your VDG to take a snapshot every 12 minutes through the CYCLE_TIME that spans over 48 hours. This practice ensures that you have 240 snapshots before the oldest nonsecure, nonpersistent snapshot is terminated.
- Set the VDG definition so that the first Snapshot at the top of the hour is secure.

Here is a sample VDG definition that may assist you with setting up your definition:

```
DEFINE VDG TESTVDG,  
    CYCLE_TIME (12, 0, SECURE, 1, 4) ,  
    MAX_SNAPSETS (240) ,  
    SRP_TERM(80) ,  
    SRP_WARN (60) ,  
    TERMINATE_POLICY (OLDEST)  
MODIFY VDG TESTVDG, ADD,  
    CCUU (770F,  
        7710, 7711)
```

This definition does the following:

- Defines a VDG called TESTVDG
- Instructs zDP to create a snapshot every 12 minutes through the CYCLE_TIME(12...)
- Secures the first snapshot and makes the next four snapshots nonsecure through the (...SECURE,1,4),
- Start rolling the oldest nonsecure snapshots off at 240

If you would like to IPL your LPAR and you did not stop zDP from running, zDP preserves the device locks for the devices in the VDG. The preservation of a device lock fails any subsequent zDP operations against those devices.

To release the device locks, perform the following:

- Get the Symmetrix ID of the devices:

```
F EMCSCF, DEV, DIS DEV (ucb)
```

- **EMCSCF** is the address space of your SCF address space.
- **ucb** is the four-digit UCB address of the device to get the Symmetrix ID for.

- Query the devices:

```
F EMCSCF, REC, QRYDLOCK, TF, DE20, 3, LCL, 030, 06
```

- **DE20** is any CUU on the array.
- **LCL** indicates any local device on the array.
- **030** is the Symmetrix ID to query.
- **06** is the starting device number.

If the device is locked, the query returns the result **SCF0723I the device is locked**.

- Free the locks on the devices:

```
F EMCSCF, REC, RELDLOCK, TF, DE20, 3, RMT, 030, 06
```

- **RELDLOCK** is the option that releases the device lock.

2.4 zDP monitoring best practices

Use the following best practices for zDP monitoring:

- To monitor the storage resource pool for your zDP/SnapVX, use the zDP ISPF panel **M;U**. **M** stands for monitor under the **VDG Functions** section. **U** is the primary command that provides **SRP Use**. (You must have an active VDG to access the Monitor panel with zDP ISPF panels). This action gives you both CKD and FBA information within the PowerMax or VMAX all-flash array.

- Option **M** from zDP ISPF panel:

```

----- zDP VDG Monitor ----- Row 1 of 1
Command=> U Refresh=> 14:29:28 09/03/20
Primary Cnds: CV = VDG CT = TGT U = SRP Use REF = Refresh
Line Cnds: S = Sel C = Cnfg M = Modify D = Delete Q = Query R = Rept
          X = Start P = Stop U = Reldlock G = Resume H = Pause F = SMF
          L = ECACLEAR Z = Create E = Export
    
```

- Option **B** from the zDP ISPF panel:

```

----- zDP SRP Monitor ----- Row 1 of 1
Command=> Refresh=> 14:25:45 09/03/20

-----Bytes-----
Ser      Tot  Tot  Snap Tot  Tot  Snap Tot  Tot  Snap Tot  Tot  Snap
Num  ID  Cap  Cap  Aloc Aloc Cap  Aloc Aloc Cap  Aloc Aloc Cap  Aloc Aloc
*****
00626 0001 10% 908M 187K  0 13M 13M  0 51T 11G  0 840G 840G  0
*****
***** Bottom of data *****
    
```

- Perform the following steps to view the snapset information:
 - In the zDP **Snapset Functions** section, select the option **1 Query**.

```

Dell EMC zDP Tool List - V 8.5

COPYRIGHT (C) 2020 Dell Inc. or its subsidiaries. All rights reserved.

Enter a command option ==>> 1

VDG Functions          TGT Functions
M Monitor              DT Display
CV Configure           CT Configure
XV Exported VDG       XT Exported TGT

Snapset Functions
1 Query

Session Control Options
S Set Options
X Exit
    
```


- b. Go to your VDG, and press **S** to select it.

```

Command===>
Primary Ccmds: REF = Refresh
  Line Ccmds:  S = Sel  Q = Query
          Serial      GK      Dev      Snap      RDP      Remote
          VDG Name    Number    CCUU    Count    Count    Util    Hop List
*****
S TESTVDG          000197600626 7D0A      2      2 1%
*****
          Bottom of data *****
    
```

- c. Go to the **CCUU**, and press the **S** that is next to it. This action provides the source device and snapset information.

```

Command===>
          CCUU  SDEV      CCUU  SDEV      CCUU  SDEV      CCUU  SDEV
-----
S 07D00 000039  _ 07D01 00003A  _ -----  _ -----
*****
          Bottom of data *****
    
```

- d. Press **F1** to review the help content, and view the **Src Trk** unique (UNI) column. This column displays the amount of space you should expect returned to the SRP if you terminate the snapset.

```

Source Cycle      Creation      Src Trk      Src Byte      Expiration
  Dev   Num   Date   Time   Chg   Uni   Chg   Uni State   Date   Time
*****
_ 000039   2 09/03/20 14:36   2K   1K   85M   32M ACT
_ 000039   1 09/03/20 14:24   2K   1K   85M   32M ACT-I 09/04/20 14:24
*****
          Bottom of data *****
    
```

- To monitor zDP Snapsets within Unisphere, one of the volumes in a VDG must reside in a Symmetrix storage group. There are two common ways to add volumes to a Symmetrix storage group:
 - Use the Mainframe Enablers functionality to align your SMS storage group to a Symmetrix storage group (reference the CREATE SYMSG command in the Dell EMC Mainframe Enablers ResourcePak Base for z/OS)
 - Identify the volume on z/OS you would like to add, and add the volume in Unisphere to an existing (or new) Symmetrix storage group.

- This example uses a volume that was in a VDG to Symmetrix group **zDP_Group**. This shows the information in Unisphere for this snapshot.

Storage Groups > zDP_Group

DETAILS | VOLUMES | PERFORMANCE | DATA PROTECTION

SNAPSHOTS | SNAPSHOT POLICIES | SRDF

Create | Modify | Restore | Link | 3 items

<input type="checkbox"/>	Snapshot	Creation Time	Linked	Restored	Expired	Secured	Snapsh...
<input type="checkbox"/>	_zDP_1281	Thu Sep 03 2020 12:49:33	—	—	—	—	zDP
<input type="checkbox"/>	_zDP_1281	Thu Sep 03 2020 12:37:33	—	—	—	—	zDP
<input type="checkbox"/>	_zDP_1283	Thu Sep 03 2020 12:25:33	—	—	—	✓	zDP

3 Space considerations

When planning for a TimeFinder SnapVX and zDP implementation, storage space is the primary resource consideration. A PowerMax/VMAX storage resource pool (SRP) is a collection of disk groups that are configured into a thin-data pool. The default setting for the PowerMax back-end SRP pool reserve capacity (PRC) is 10%. When space consumption reaches the PRC (which is strictly used for new host writes), you cannot create snapshots, and existing nonsecure snapshots are failed. Due to this behavior, all SnapVX and zDP implementations should accommodate for at least some of the snapshots to be secure.

When the SRP is 100% full, SRDF replication stops if the array is an SRDF target. Also, all local host I/O stops, which has an operational impact. It is critical to design proper space alerting to warn customers well before the 90% SRP full is reached. Space-reclamation procedures should be well understood, tested, and documented to relieve the space shortage condition should they arise.

Space-reclamation procedures include the following:

- Terminating nonsecure snapshots
- Linking a more-recent snapshot with fewer snapshot deltas
- Issuing a free command to an unused snapshot target
- Running thin reclaim utility (TRU), which returns space to the SRP from a host perspective

4 Deploying local-array SnapVX and zDP

SnapVX and zDP run in the SCF address space that is delivered by Mainframe Enablers software. The SCF address space runs on a z/OS LPAR. This SCF address space has connectivity to the PowerMax (or VMAX all-flash array) through gatekeeper devices. Besides the space consumption-risk that is mentioned previously in this paper, the primary consideration when using SnapVX and zDP on the local (DC1) storage environment is the host performance impact. Snapshot creation is not free from a z/OS-host-response-time perspective. Even though snapshot intervals may be as short as five minutes, it may be preferable to use rolling small-interval snapshots for cyber protection in a remote-array (DC2) deployment. The ideal environment for the local array (production site) includes daily full-volume backup applications. In this environment, the snapshot only ages for 24 hours before it can be terminated after the backup has completed. Typically, the space usage is far lower than a full clone would require.

There are two main reasons to implement SnapVX and zDP locally (DC1 environment):

- Protection against a massive cyber event
- To surgically LINK the snapshot or zDP snapset to a subset of target volumes to recover data

TimeFinder SnapVX can be used selectively to link a subset of the volumes in a zDP snapset using the ZDP(YES) parameter in the TimeFinder SnapVX LINK job. This practice provides another option to surgically select volumes to recover data from.

5 Deploying remote-array TimeFinder SnapVX and zDP

Customers can use SnapVX and zDP to support traditional disaster recovery (DR) testing at the DR site which formerly used full volume copies (clones or BCV). The DR testing is adequately supported with a MODE(NOCOPY) pointer-based link which is space-efficient. Ideally, the DR test should not affect the rolling protection of zDP during the test. A linked snapshot for the DR test consumes space as the snapshot ages. You should determine how long a DR test snapshot needs to live to accurately plan the space consumption.

There are multiple reasons why the DR site array can be used for short-interval SnapVX zDP cyber protection. You can IPL (for testing purposes) the entire set of volumes in your DR test LPARs. Also, the consequences of an array SRP reaching unsafe operational levels are much lower if the snapshots are in the SRDF distance array. SRDF replication protection may be at risk, but host outages that are due to the SRP being 100% full are impossible if the snapshots are in the distance array.

You can create SnapVX snapshots and zDP snapshots in remote arrays that are connected by SRDF by using a local instance of Mainframe Enablers software that is running on a z/OS LPAR. TimeFinder SnapVX can communicate with the remote array. The RMT (remote) parameter with CREATE, LINK, UNLINK, and TERMINATE functions enable controlling snapshots on the remote array.

With zDP, when the VDG and TGT constructs are created at the local (production) site using Mainframe Enablers, use the MODIFY command to ADD devices and populate the VDG or TGT. Using the RMT(GP) parameter in the MODIFY, ADD device list allows you to create zDP snapshots at the array that is attached to the remote array in SRDF group GP (in the example above). This configuration method is deployed when there is no active z/OS LPAR running at the DR site.

The host-performance impact that is mentioned in section four does not apply if the SRDF replication method is synchronous. If the replication is synchronous mode, this configuration causes a host-performance impact (ECA enabled) if you create a consistent snapshot of an SRDF R2 group. If the replication method is SRDF/Asynchronous, ECA is not required, and the host impact at the production site is negligible.

6 Secure snapshots

Secure snapshots survive the previously mentioned SRP full events that compromise nonsecure snapshots. At 90% SRP full, all new snapshot creation, whether secure or not, stops. SnapVX-created snapshot jobs fail, and zDP stops. Worse, at 90% SRP usage, the array fails any existing nonsecure snapshots as it sacrifices snapshots to keep host I/O or SRDF functioning. Secure snapshots are not failed.

Nonsecure snapshots exist indefinitely until they are terminated. If zDP stops or is stopped, the existing snapshots are not terminated until zDP is restarted. Secure snapshots behave differently. The secure attribute is specified at creation time, but you can also add it after the snapshot is created. The unit of time that a snapshot must exist is measured in days. When it is associated with an expiration date and time, the snapshot cannot be terminated. Also, the snapshot cannot be destroyed by a command or by an array-full condition as mentioned previously. Secure snapshots expire, but they are not terminated. For example, if zDP stops or is stopped on Friday, and zDP was creating secure snapshots with a time to live of two days, on Monday, all zDP snapshots are expired. This behavior means that it is more important to monitor zDP more closely if secure snapshots are being created to avoid having gaps in snapshot protection.

Secure snapshots behave like nonsecure snapshots and can be linked and unlinked, but they cannot be terminated. Secure snapshots that are in a linked status can expire, but they do not terminate while they remain linked. When a secure expired snapshot is unlinked, it is terminated. Secure snapshots do not change the space consumption of a snapshot. Changes made to the snapshot source accumulate SRP space, and this behavior is no different than nonsecure snapshot behavior. This operational difference is present because secure snapshots cannot be terminated if an SRP space shortage becomes critical. The sizing headroom should be more conservative when planning for secure snapshots.

zDP can SKIP intervals of secure snapshots to easily provide a mix of secure and nonsecure snapshots using the CYCLE parameter. The following example shows a VDG definition that specifies snapshots taken every hour for 48 hours, and every other snapshot is secure with a lifespan of 2 days.

```
CYCLE_TIME (12, 0, SECURE, 1, 4) ,
```

The SKIP feature (represented by 4 in the above cycle definition) was developed to enable reclaiming SRP space by terminating nonsecure snapshots, should SRP space usage reach critically low levels. If zDP stops at any time, the nonsecure snapshots remain indefinitely which reduces the risk of losing cyber protection. Be careful when using the SKIP parameter and choose a value that is consistent with the secure lifespan expiration. As a best practice, use the following formula:

$$\text{SNAPSHOT INTERVAL MIN} * \text{MAX_SNAPSETS} / 60 \text{ MIN PER HR} = \text{AGE OF OLDEST SNAPSHOT (HRS)}$$

The age of the oldest snapshot should be an even number of days so that zDP terminates nonsecure snapshots at the same frequency as the secure snapshot expiration.

Here is an example of a definition that may cause issues:

$$10 \text{ MIN INTERVAL} * 256 \text{ MAX_SNAPSHOTS} / 60 = 42.7 \text{ HOURS which is not an even multiple of days.}$$

A more suitable definition would be as follows:

$$12 \text{ MIN INTERVAL} * 240 \text{ MAX_SNAPSHOTS} / 60 = 48 \text{ HOURS with a two day SECURE attribute.}$$

7 Operational best practices

We recommend the following zDP operational best practices:

- Define a zDP VDG that aligns with the SRDF groups. With SRDF groups, only create groups if required since it is easier to manage fewer groups.
- Always use the NOSORT attribute when creating and adding devices (MODIFY,ADD) to the VDG and TGT to avoid zDP changing the SOURCE to TARGET pair relationship. Specify NOSORT to ensure that zDP maintains the required SOURCE to TARGET mapping. Without NOSORT, zDP does not always obey the specified sequence of devices that are added to the VDG and TGT. The result could cause unpredictable UCB mapping. Not following this process can cause confusion that the RES volume is at one UCB, while it resides at a different UCB address.
- While zDP is active within SCF, SRDF actions (SC commands) are blocked because zDP puts a lock on the devices. Stop zDP to perform host-component SC commands. A sample stop command is as follows:

```
`/F <scf address space>,ZDP STOP <vdg name>'
```

- With Mainframe Enablers versions before 8.4, zDP definitions do not persist beyond IPLs. The snapshots persist, but the VDG and TGT definitions and device lists do not. These definitions must be re-created and MODIFIED, and devices must be ADDED after an IPL. As of Mainframe Enablers 8.5, customers can preserve the zDP VDG and TGT definitions to avoid having to re-create and modify VDGs and TGTs after an IPL. If you have Mainframe Enablers 8.4 or lower stop zDP before performing an IPL for the controlling LPAR and re-creating the VDG and TGT definitions.

8 Summary

SnapVX and zDP for mainframe local replication technology was introduced with the VMAX3™ generation of the Symmetrix family in early 2016. Before VMAX3 local replication was full volume BCV or clones that largely restricted customer usage to one or two local copies. Initially, SnapVX allowed a maximum of 256 snapshots of a device. As of 2019, the number of SnapVX snapshots per device is enhanced to allow up to 1,024 snapshots. Today, we see customers using TimeFinder SnapVX snapshots and zDP Snapsets for these business reasons:

- Traditional disaster recovery site point in time (PIT) copy for DR testing
- PIT copy for full volume backups
- Rolling small interval snapshots for cyber protection

Implementation of zDP can provide a level of protection from pervasive logical corruption that was previously unavailable to mainframe users. Having a copy of data available that was close to the point of corruption enables rapid recovery and faster resumption of normal processing. Data restoration from tape media can be eliminated, and recovery processing can be performed far more rapidly as very recent data can be utilized in the recovery process.

zDP has helped to usher in a new discipline within business continuity planning: cyber recovery. Like its cousin, disaster recovery, cyber recovery utilizes additional copies of data to provide business value but does so to provide protection from a new risk, cyberattack. zDP was the first product to provide this protection and solutions to aid in rapid recovery will continue to evolve to meet the ever-evolving need for business continuity.

A Technical support and resources

[Dell.com/support](https://www.dell.com/support) is focused on meeting customer needs with proven services and support.

[Storage and data protection technical white papers and videos](#) provide expertise that helps to ensure customer success with Dell EMC storage and data protection platforms.