DS8000 Security Reference Architecture

Nick Clayton, Yang SH Liu, Harry Yudenfriend

Abstract

The IBM DS8000 Storage System® is IBM's premier enterprise class storage system supporting both distributed systems and mainframe FICON attachment. To aid clients in providing a robust and secure storage infrastructure for use by servers, the DS8000 has delivered a number of functions that simplify this task. This paper describes the storage security capabilities of the DS8000 including the most recent advancements in storage security functions and the value they provide clients.

Introduction

Most organizations cite data protection as their most important security issue. Typical concerns include how data is stored and accessed, compliance and audit requirements, and business issues that involve the cost of data breaches, notification requirements, and damage to brand value. All sensitive or regulated data, including archived data, needs to be properly segregated on the cloud and shared storage infrastructure.

According to the Ponemon Institute© Research report, 2017 Cost of Data Breach Study[1], the average cost for each lost or stolen record containing sensitive and confidential information is $141 in this year's study. Companies are experiencing larger breaches than in past years where the average size of the data breaches has increased 1.8 percent from last year. Data security breaches of client data is expensive because of fraud, the damage to a company's reputation harms business growth and the inability to protect data from destruction threatens the continued existence of the company. Businesses require consumable, cost effective policy based approaches to data security.

This whitepaper describes the most recent mechanisms put into place for the DS8000 family of storage systems to help enterprises protect their data. For example, Logical Corruption Protection helps clients recover from attacks on their data. Resource Groups provides a multi-tenant security capability that allows clients to specify policy to restrict the use of replication functionality to predefined groups of devices. Clients choosing to deploy host based dataset and file encryption capabilities have to consider the ramifications on other parts of the SAN infrastructure.

Protecting user data on the DS8000

Logical Corruption Protection

Many organizations are becoming increasingly concerned about the risk of deliberate attacks against enterprise data which could result in this data being logically corrupted or otherwise made unusable. Continuous replication functionality such as Metro Mirror or Global Mirror does not provide any protection from this type of event or indeed from other inadvertent corruption of

[1] "2017 Cost of Data Breach Study, Global Overview", Ponemon Institute Research Report, Sponsored by IBM Security , June 2017

data. In fact, replication functions will quickly propagate host caused data corruption to all copies as to the storage this is simply another update IO. Hence many organizations are looking at providing one or more Point in Time copies of data using FlashCopy functionality to provide an ability to quickly access this data if required. Multiple copies would provide an ability to restore back to different points in time providing a detection time window for any problem and the copies would be deliberately isolated to increase security.

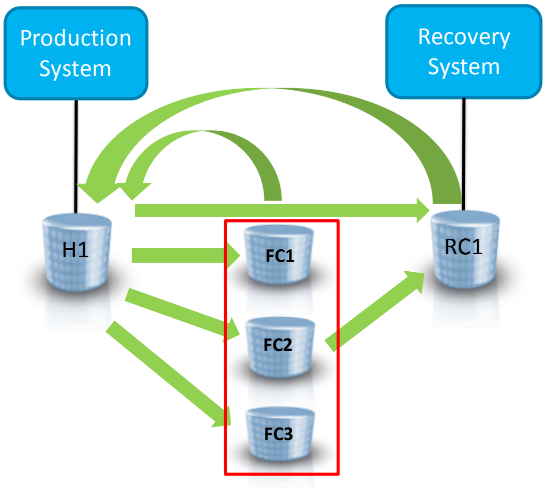
If a logical corruption event was to occur then there are a number of strategies that could be used to recover from this:

The first would be what is referred to as a **catastrophic recovery** scenario where the data from the previous point in time is restored and production services are restarted from this copy. However, in a large environment there are probably many scenarios where only a subset of the data and applications are affected and so the catastrophic recovery scenario is not appropriate.

In this case, the first action might be to restart a system from one of the previous Point in Time copies or from a copy of the current data. This can then be used to perform **forensic analysis** of the data and determine what action to take.

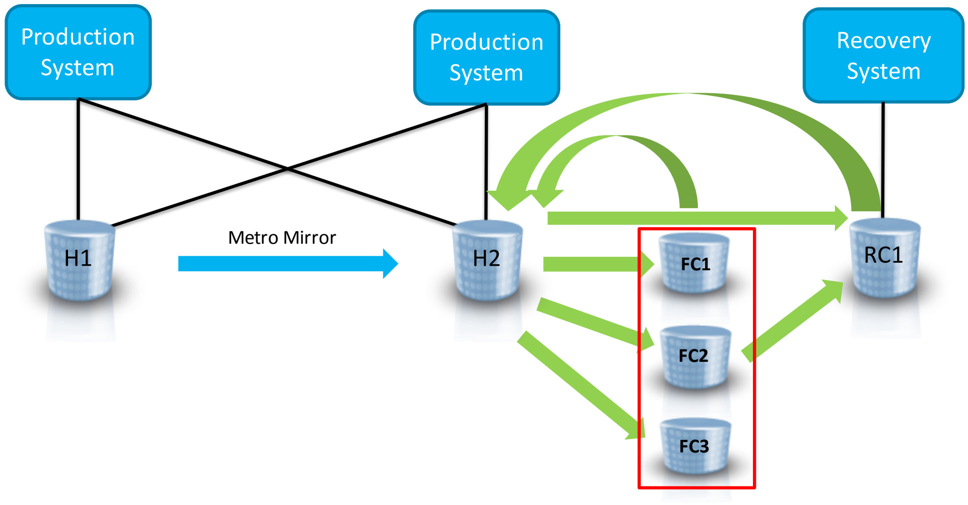
Following this analysis, it might be decided to perform a **surgical recovery** of the data either from normal backups or from one of the Point in Time copies

In order to handle these various scenarios a FlashCopy topology similar to the one below is recommended to be implemented where there are a number of FlashCopies taken from either a production device or from a replicated copy. The Cascaded FlashCopy functionality delivered in R8.3 of the DS8000 microcode provides an ability to restore any one of these copies to the production device while maintaining the other flash copy relationships. Cascaded FlashCopy also allows any of the copies to be FlashCopies on to a designated recovery copy which could be used for forensic analysis and surgical recovery.

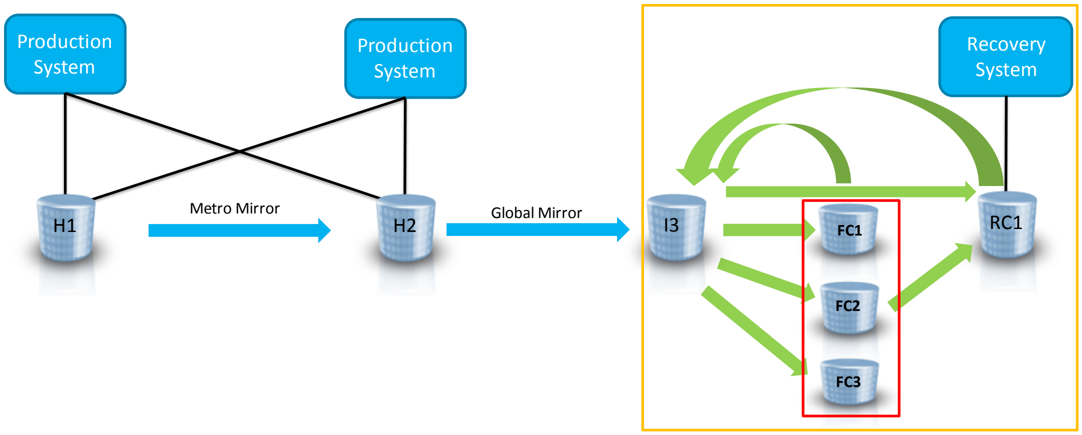


The Logical Corruption protection copies could be taken on a storage systems in the existing HA/DR topology or additional isolated storage systems could be installed in some location to provide a more isolated copy to increase security

For example, the diagram below shows additional Logical Corruption Protection copies added to the secondary storage system in a Metro Mirror environment



The diagram below shows an additional storage system installed in an isolated environment using Global Mirror to replicate the data and then taking the Logical Corruption Protection copies from this.



Given the assumption that there may have been a deliberate attack resulting in the corruption or destruction of data, it is also necessary to consider the possibility that the attacker also attempts to destroy all logical copies of the data as well as the primary copy. There are a number of strategies that are suggested in order to reduce these risks:

- Avoiding host access to the copies of data so that a compromised host cannot be used to destroy both the production data and the copies. This can be done for CKD devices by not defining the target devices in the IODF and for FB devices by not defining them to a host on the DS8000. It is also possible to write inhibit a FlashCopy target in the DS8000 so that even if a host obtained access only reads would be allowed

- Minimizing the administrative access to the storage systems containing the copies of data by using some type of “break glass” approach to avoid day-to-day access with full admin rights

- Taking the copies of data on an additional storage system with additional physical and logical isolation and adding further security restrictions compared to other systems such as restricted network access, isolated SAN connectivity, reduced number of users with userids.

Using DS8000 Encryption of Data at Rest

The IBM DS8000 has supported encryption of data at rest for a number of years. Encryption of data at rest is accomplished by support of encryption-capable hard disk drives (HDDs) and flash drives. These Full Disk Encryption (FDE) drive sets are used with key management services. Using drive level encryption means that there is no performance penalty in terms of I/O service time to the use of encryption. However, use of encryption technology involves several considerations that are critical for you to understand to maintain the security and accessibility of encrypted data.

> https://www.ibm.com/support/knowledgecenter/en/HW213_7.4.0/com.ibm.storage.ssic.help.doc/f2c_ds8000encryption_3ekm6r.html

Recent enhancements to the DS8000 includes the exploitation of the IBM Security Key Lifecycle Manager Version 2.6, the introduction of “Gemalto SafeNet KeySecure”, which supports the Key Management Interoperability Protocol (KMIP) with the DS8000 Release V8.1 code and an updated GUI for encryption functions.

> IBM DS8880 Data-at-rest Encryption,
> http://www.redbooks.ibm.com/redpapers/pdfs/redp4500.pdf

Decommissioning DS8000 and Secure Data Overwrite

IBM Certified Secure Data Overwrite (SDO) is a process that provides a secure overwrite of all data storage in a DS8880 storage system. The SDO process is initiated by the IBM service support representative (SSR) after all logical configuration information and encryption groups have been removed. The process may continue for a full day, unattended, until it completes.

The certificate provides written verification, by drive or Flash Card serial number, of the full result of the overwrite operations. You can retrieve the certificate by using DSCLI, or the IBM SSR can offload the certificate to removable media, and provide the media to you.

> IBM DS8880 Architecture and Implementation (Release 8.2.1),
> http://www.redbooks.ibm.com/redbooks/pdfs/sg248323.pdf, pages 19 and 95

Using Host Based Encryption

The use of host based encryption of z/OS data sets and distributed systems files can enhance security by enforcing policy based authentication for access to the data and protecting the data while in flight through the SAN. The use of host based encryption improves data security without requiring expensive modifications to existing applications to add encryption.

z/OS Dataset Encryption

With z/OS data set encryption, you can encrypt data without requiring application changes.

“DFSMS Using Data Sets z/OS Version 2 Release 3”, pages 66-71, SC23-6855-30, July 17, 2017
https://www-304.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R3sc236855/$file/idad400_v2r3.pdf

z/OS data set encryption, through SAF controls and RACF® or equivalent function along with SMS policies, allows you to identify new data sets or groups of data sets to be encrypted. You can specify encryption key labels to identify encryption keys to be used to encrypt selected data sets. The specified key label and encryption key must exist in the ICSF key repository (CKDS). With data set encryption, you are able to protect data residing on disk from being viewed by unauthorized users in the clear. Authorization is based on access to the key label that is associated with the data set and used by the access methods to encrypt and decrypt the data.

z/OS data set encryption provides the ability to encrypt sequential extended format data sets, accessed through BSAM and QSAM, and VSAM extended format data sets (KSDS, ESDS, RRDS, VRRDS, LDS), accessed through base VSAM and VSAM RLS. Encrypted data sets must be SMS-managed extended format. They also can be compressed format.

V2.2 DFSMS Using Data Sets publication:
http://publibz.boulder.ibm.com/zoslib/pdf/OA50569.pdf

V2.3 DFSMS Using Data Sets publication:
https://www-304.ibm.com/servers/resourcelink/svc00100.nsf/pages/zOSV2R3sc236855/$file/idad400_v2r3.pdf

Importance of Host Based Compression

It is recommended that clients using host based encryption also exploit host based compression prior to the encryption of the data. If the data is not compressed prior to the encryption there could be consequences to other parts of the client infrastructure. For example, replicated data that is being compressed in the SAN infrastructure by DWDM technology will no longer be effective trying to compress encrypted data. Without compressing prior to the encryption of the data, additional bandwidth maybe be required to meet the same service level agreements. Another example maybe that tape systems may require additional capacity in terms of disk space, in the case of virtual tape, or tape cartridges. If deduplication of data is supported, host encryption could prevent dedupe from working. Additionally, DASD storage systems depending on compression in the storage system may require additional capacity as encrypted data does not compress well.

For z/OS clients, the IBM z Systems platform has an I/O adapter that compresses and decompresses data using the industry-standard Deflate algorithm. Supported by the zEnterprise Data Compression (zEDC) feature of z/OS V2.1 and above, the zEDC Express[2],[3] adapter is optional with the IBM Z servers. It can compress data at more than 1 GB per second while using roughly 100 times less CPU than software implementations of the same algorithm.

"New zEDC Express Adapter Compresses Data Faster While Using Less CPU", IBM Systems Magazine, September 2013, http://www.ibmsystemsmag.com/mainframe/trends/IBM-Announcements/zedc_compression/

"Reduce Storage Occupancy and Increase Operations Efficiency with IBM zEnterprise Data Compression", International Technical Support Organization, SG24-8259-00, February 2015, http://www.redbooks.ibm.com/redbooks/pdfs/sg248259.pdf

Encryption for Distributed Systems

IBM Spectrum Scale is a high-performance enterprise platform for optimizing data and file management.

An introduction to IBM Spectrum Scale, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=DCW03057USEN

Spectrum Scale simplifies data management with integrated tools designed to help organizations manage petabytes of data and billions of files as well as control the cost of managing these ever-growing data volumes. Long considered a pioneer in big data storage, IBM focuses on advanced storage technologies that enable companies to store large quantities of file data. Spectrum Scale continues this tradition and marks a significant milestone in the evolution of big data management. Part of the IBM Spectrum Storage™ family, Spectrum Scale 4.1 introduces revolutionary new features that clearly demonstrate the IBM commitment to providing groundbreaking storage solutions, including file encryption and secure erase.

IBM Spectrum Scale™ V4.2 adds file compression to reduce the size of data at rest. File compression is intended primarily for cold data and favors saving space over access speed. File compression can be driven by policies that enabled administrators to compress only files that are not accessed for some specified time. Data is decompressed inline for each read access.

IBM Spectrum Scale 4.2.1, https://www.ibm.com/support/knowledgecenter/en/STXKQY_4.2.1/com.ibm.spectrum.scale.v4r21.doc/bl1adm_compression.htm

Clients using the file encryption capabilities of Spectrum Scale need to consider the effects on

[2] Anthony Sofia, Cecilia Carranza Lewis and Peter Sutton, "New zEDC Express Adapter Compresses Data Faster While Using Less CPU", IBM Systems Magazine, September 2013

[3] Paolo Bruni, Maria Kroos Boisen, Gianmauro De Marchi and Franco Pinto, "Reduce Storage Occupancy and Increase Operations Efficiency with IBM zEnterprise Data Compression", International Technical Support Organization, SG24-8259-00, February 2015

the SAN and storage systems used to hold the data (see Importance of Host Based Compression above).

DS8000 User Security

User Security Basics

When the administrator adds a user, the administrator enters a password. During the user’s first login, this password must be changed. Password settings include the time period (in days) after which passwords expire and a number that identifies how many failed logins are allowed. The user ID is deactivated if an invalid password is entered more times than the limit. Only a user with administrator rights can then reset the user ID with a new initial password

Role Based Security

DS8880 supports different user roles in order to help you manage secure authorization, which specifies the resource and access for different users. A user can be assigned to more than one group. The following roles exist:

- The Administrator (admin) has access to all Hardware Management Console (HMC) or Management Console (MC) service methods and all storage image resources, except for encryption functions. This user authorizes the actions of the Security Administrator during the encryption deadlock prevention and resolution process.

- The Security Administrator (secadmin) has access to all encryption functions. This role requires an Administrator user to confirm the actions that are taken during the encryption deadlock prevention and resolution process.

- The Physical operator (op_storage) has access to physical configuration service methods and resources, such as managing the storage complex, storage image, rank, array, and extent pool objects.

- The Logical operator (op_volume) has access to all service methods and resources that relate to logical volumes, hosts, host ports, logical subsystems, and volume groups, excluding security methods.

- The Monitor group has access to all read-only, non-security MC service methods, such as the list and show commands.

- The Service group has access to all MC service methods and resources, such as running code loads and retrieving problem logs. This group also has the privileges of the Monitor group, excluding security methods.

- The Copy Services operator has access to all Copy Services methods and resources, and the privileges of the Monitor group, excluding security methods.

- No access prevents access to any service method or storage image resources. This group is used by an administrator to deactivate a user ID temporarily. By default, this user group is assigned to any user account in the security repository that is not associated with any other user group.

DS8870 Authentication
https://www.ibm.com/support/knowledgecenter/HW213_7.1.0/com.ibm.storage.DS8000.learning/authentication_script.html

IBM DS8880 Architecture and Implementation (Release 8.2.1), http://www.redbooks.ibm.com/redbooks/pdfs/sg248323.pdf, Chapter 10.2, page 246.

Remote Authentication with LDAP

The IBM System Storage DS8000® allows for user authentication from an external source. Often a lightweight directory access protocol, or LDAP, server serves as this external source.

Lightweight Directory Access Protocol (LDAP) authentication support, which allows single sign-on (SSO), can simplify user management by allowing the DS8000 to rely on a centralized LDAP directory rather than a local user repository. LDAP can be enabled through the Copy Services Manager (CSM), which is packaged with the HMC code.

Consider the integration of Lightweight Directory Access Protocol (LDAP) to allow a single user ID and password management. With Release 8.1, you can take advantage of the LDAP capability offered by the Copy Service Manager residing on the Hardware Management Console (HMC).

IBM DS8880 Architecture and Implementation (Release 8.2.1), http://www.redbooks.ibm.com/redbooks/pdfs/sg248323.pdf

IBM DS8880 Integrated Copy Services Manager and LDAP Client on the HMC, REDP-5356: http://www.redbooks.ibm.com/abstracts/redp5356.html

Two factor authentication for HTTP access

The DS8000 does not itself offer two factor authentication for either the GUI or DSCLI access. However it is possible to create an environment in which a prior two factor authentication process is required before a user can access these user interfaces.

Many organizations restrict the systems which are able to access the DSCLI on the DS8000 HMCs using firewall rules to prevent access from all but a small set of systems. If these systems are secured by two factor authentication then any user of the DSCLI must have first passed through this process before using the DSCLI. As the DSCLI is now available on z/OS as part of the CSM for z/OS software it is possible to use a z/OS system for this purpose and take advantage of the two factor authentication capabilities of this platform.

The DS8000 user interface is accessed via a browser and hence it is also possible to use similar firewall capabilities to require a two factor authentication before being allowed to access the DS8000 HMC via HTTP.

Network security for DS8000

The DS8000 uses a private internal network for communication between the DS8000 processor nodes and the HMC servers. All administrative access is through the network ports on the HMC servers.

HMC 860 Connectivity Security White Paper
http://www-01.ibm.com/support/docview.wss?uid=isg3T7000236&aid=1

Transparent Cloud Tiering Security

Transparent Cloud Tiering for DS8000 is a feature in conjunction with z/OS® and DFSMShsm that provides server-less movement of archive and backup data directly to an object storage solution. Offloading the movement of the data from the host to the DS8000 unlocks DFSMShsm efficiencies and saves z/OS MIPS. Instead of traditional tape volumes that HSM and DSS have used before, Transparent Cloud Tiering migrates data at the data set level to the object store. By using this method of storage capability, DFSMShsm can bypass many tape-centric architectural guidelines. It also removes the need for activities such as Recycle, 16K block sizes and serial access.

If the Transparent Cloud Tiering functionality is used then there are additional network interfaces on the DS8000 processor nodes that must be connected to a network with access to the object storage devices used to store and retrieve data. These network interfaces are protected by a firewall and do not have any additional services enabled on them, being used for outbound connections only.

Transparent Cloud Tiering can use SSL or TLS for authentication using user provided certificates if desired. However, the data sent from the DS8000 to the Cloud Storage systems is not encrypted and so a VPN connection should be used if this is to be sent over external networks.

IBM DS8880 Transparent Cloud Tiering,
https://www.ibm.com/support/knowledgecenter/en/HW213_7.5.0/com.ibm.storage.ssic.help.doc/f2c_trans_cloud_tiering.html

Remote Support Security

IBM provides remote support capabilities for the DS8880. The remote support enables the storage to communicate with IBM, and allows IBM support to remotely connect to the system when authorized by the user. The benefits of the remote support are that IBM Support can respond quickly to events reported by you or the system.

IBM has taken many steps to provide secure network access for the Management Console. The client can define how and when the IBM SSR can connect to the Management Console. When remote support access is configured, IBM Support can connect to the Management Console to start problem analysis and data gathering.

Remote support access and actions are also included in the DS8000 audit log described later in this document.

With the DS8880 two inbound connectivity options are available:

- Assist On Site (AOS) either embedded or through an external AOS Gateway
- Remote Support Center

Assist On Site (AOS) for remote support access

AOS is an embedded feature, on DS8700, DS8800, DS8870, and DS8880 and is preinstalled and customized on the Management Console.

It is also possible to configure AOS using an external gateway which provides a centralized access point for IBM support across multiple DS8000s or other IBM Storage Systems.

Remote Support Center (RSC) for remote support access

Starting with R8.1 the DS8000 HMC has also been enabled to use the Remote Support Center management system to provide support access to the DS8000 Management Console.

This is a SSH based remote service solution which can be used in cases where AOS does not meet the local security standards and will over time replace the AOS solution and become the common support access solution for IBM Storage Systems.

> IBM DS8880 Architecture and Implementation (Release 8.2.1), http://www.redbooks.ibm.com/redbooks/pdfs/sg248323.pdf,
>
> IBM Assist On-site for Storage Overview, https://www.redbooks.ibm.com/redpapers/pdfs/redp4889.pdf

z/OS Security for DS8000 advanced function

If a z/OS host has access to a device on the DS8000 through the IODF then the DS8000 relies on the host operating system to provide security on any commands that are issued to the device.

There is no additional authorization checking within the DS8000 for commands issued over FICON interfaces. One exception to this is when the resource group functionality (discussed later in this paper) is being used to restrict the target devices that can be used when replicating one device to another.

The z/OS system itself is protected by RACF or other similar security products and these have recently begun to introduce multi factor authentication to provide additional security in addition to the user password. IBM Multi-Factor Authentication for z/OS currently supports the use of RSA® SecurID® Tokens, including hardware-based or software-based tokens and IBM has also issued a statement of direction for additional future authentication factors. The solution also provides an audit trail using SMF records.

IBM System Magazine, IBM Multi-Factor Authentication for z/OS Helps Maintain a Secure Infrastructure, http://www.ibmsystemsmag.com/mainframe/administrator/security/Multi-Factor-Authentication

IBM Multi-Factor Authentication for z/ OS V1R2, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSS03139USEN

Once the user is logged on to the z/OS system then access for the user to Copy Services functionality on the DS8000 is controlled using a comprehensive set of RACF Facility Classes. There are typically two profiles for each function, the first one providing query (read only) access and the second allowing for control of the replication functionality. For example, for Metro Mirror and Global Copy we have

- STGADMIN.ANT.PPRC.CQUERY
- STGADMIN.ANT.PPRC.COMMANDS

This enables a security administrator to provide a specific level of access to each user or set of users. The DFSMS Advanced Copy Services manual provides more details on RACF facility classes for DS8000 functionality.

DFSMS Advanced Copy Services, https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.2.0/com.ibm.zos.v2r2.idag200/advcop2.htm

Multi-tenancy security features

Different aspects of Multitenancy - administrative vs user access

The DS8000 does not support the ability to logically divide a DS8000 from an administrative perspective. Therefore a user with admin access to a DS8000 can manage all the logical resources on the storage system. However many organizations do use the DS8000 with multiple tenants but have a single central organization with the admin access.

Resource Groups

The DS80000 provides a multi-tenant security capability referred to as Resource Groups[4].

Resource Groups enables policy-based limitations on DS8000 copy services by allowing the definition of multiple groups of volumes and restrict the use of replication functionality to within these defined groups. This partitioning capability is used by clients to isolate various subsets of the environment as though they are separate tenants. This capability can be used to separate mainframe data from distributed data, Windows from Unix, or accounting department applications from marketing applications. In this way a z/OS tenant can be restricted to only perform replication functionality within their assigned volumes and cannot inadvertently or maliciously copy or overwrite another tenant’s data.

Resource groups offer an enhanced security capability that supports hosting multiple customers with copy services requirements and the single customer with requirements to isolate the data of multiple operating system environments.

Resource groups introduce the logical separation of DS8000 resources and offer these benefits:

- Enable the secure use of Point-in-Time copy (FlashCopy) functions by multiple clients that are hosted on a single shared DS8000 storage system, where Point-in-Time copy functions are restricted to the resources (volumes) within each client’s domain.

- Enable the secure use of Remote Mirror and Copy functions by multiple clients that are hosted on shared primary, secondary, and tertiary DS8000 storage systems to perform controlled data migration and disaster recovery.

Resource groups for clients offer these benefits:

- Provides additional security to prevent other users of a shared infrastructure from accidentally or deliberately using replication functionality to overwrite data

- Enables greater sharing of the DS8000 resources to help reduce cost pressures for clients

[4] Bert Defrasne, Roland Wolf, IBM System Storage DS8000 Copy Services Management and Resource Groups, REDP-4758-01, January 2013

in that it allows them to buy only what they need

- Offers greater flexibility to provide capacity on demand to clients who are unable to forecast capacity needs accurately and have requirements to rent capacity during peak usage periods during their business year

Resource groups for service providers offer these benefits:

- The ability to drive up utilization of primary, secondary, and tertiary site storage through secure sharing of the infrastructure and the ability to drive down the total cost of ownership (TCO) through sharing techniques

- The ability to offer capacity on demand with high-availability copy services functions to their clients

When the IT infrastructure is managed by a service provider, the overall administration of resource groups for a storage system should be owned and managed by the service provider, with subordinate administrator roles defined to each hosted client or tenant’s subdomain. Ownership of the subordinate Copy Services operator roles can be with either the service provider or the client, depending on how much control the client wants to retain.

For the single client that operates in a multiple operating systems environment, resource groups provide more data protection against inadvertent human errors or deliberate malicious acts through the use of Copy Services functions.

“IBM System Storage DS8000 Copy Services Management and Resource Groups”, REDP-4758-01, January 2013,
http://www.redbooks.ibm.com/redpapers/pdfs/redp4758.pdf

Multi-tenant replication management with CSM

IBM Copy Services Manager includes the concept of an Operator user role which only has authority over the sessions to which they have been granted access to. In this way a tenant of an environment can be enabled to control the replication function for their particular environment without being able to control other environments on the same DS8000.

IBM Copy Services Manager V6.1.5, Users Roles, https://www.ibm.com/support/knowledgecenter/SSESK4_6.1.5/com.ibm.storage.csm.help.doc/frg_c_user_roles.html

IBM System Storage DS8000 Copy Services Scope Management and Resource Groups, http://www.redbooks.ibm.com/redpapers/pdfs/redp4758.pdf

Resource groups for Copy Services scope limiting, https://www.ibm.com/support/knowledgecenter/en/ST5GLJ_8.2.3/com.ibm.storage.ssic.help.doc/f2c_rgsscopelimiting_1kt6br.html

Alerting and logging

DS8000 Audit Log

The DS8880 offers an audit log. The audit log is an unalterable record of all actions and commands that were initiated by users on the storage system through the DS8000 Storage Management graphical user interface (GUI), DS8000 Command Line Interface (DSCLI), DS8000 Network Interface (DSNI), or Copy Service Manager (CSM). The audit logs can be exported and downloaded by the DS CLI or Storage Management GUI and can also be offloaded via a syslog service.

Monitoring DS8000 Events and Audit logs via syslog service

With increased security requirement, clients may use a central audit system and require DS8000 to send the events and logs to a central repository. Starting from DS8000 Release R8.1, users can configure up to 8 syslog servers on DS8000, and the events and audit logs of DS8000 are sent to those servers automatically and securely.

The following type of data are sent to customer's configured syslog servers:

1. DS8000 Audit logs:

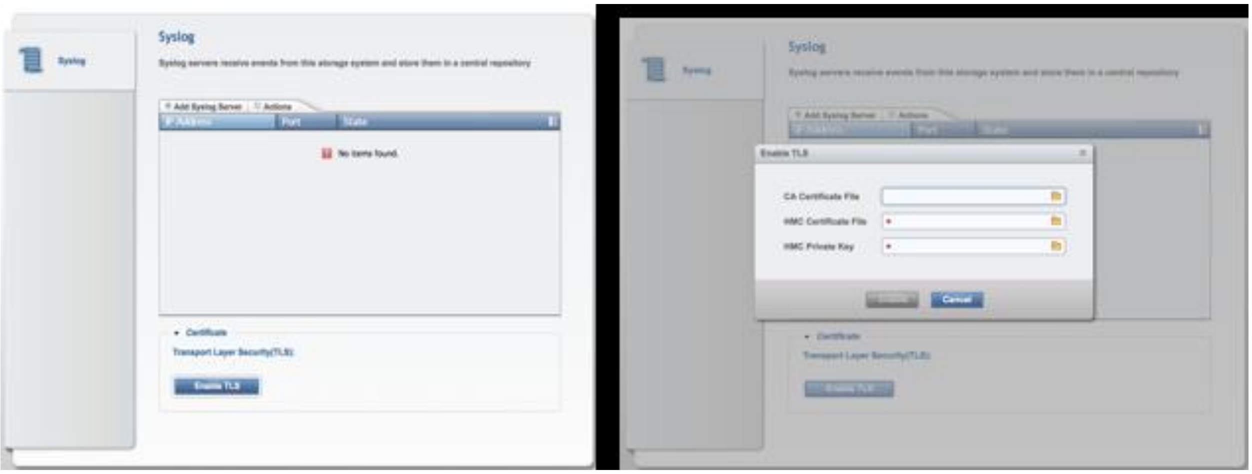
Including every user login/logout events, all commands issued by using the GUI and DSCLI while the user is logged in, and remote access events.

2. DS8000 Events (available since R8.2):

Including all the DS8000 informational/warning/error events reported on GUI today.

3. All "/var/log/messages" entries on HMC (available since R8.2).

To make sure the data is securely transferred to syslog servers, customer can enable TLS for the data transfer to syslog servers via DSGUI and DSCLI. For the TLS enablement, customer need to specify the certificate authority (CA) certificate file, the storage system certificate signed by the CA (HMCCertificatefile), and the private key for the storage system (HMCPrivateKey).



Syslog servers receive events from this storage system and store them in a central repository

No items found.

```
$dscli> mksyslogserver -addr 9.110.75.7 -protocol tls -cacert
/Users/heping/ut/syslog/ca.pem -hmccert /Users/heping/ut/syslog/cert.pem -key
/Users/heping/ut/syslog/key.pem test
Date/Time: September 25, 2016 8:28:21 PM MST IBM DSCLI Version: 7.8.20.148 DS: -
CMUC00508I mksyslogserver: The syslog server machine.example.net has been created.

$dscli> lssyslogserver -l
Date/Time: September 25, 2016 8:28:54 PM MST IBM DSCLI Version: 7.8.20.148 DS: -
name IP address port state  access protocol type                HMC
=================================================================
test 9.110.75.7  514 active online tls      audit,message,event 1
test 9.110.75.7  514 active online tls      audit,message,event 2
```

z/OS audit logging

Advanced function commands issued to the DS8000 from z/OS systems can use the RACF logging and reporting functionality to identify users successfully or unsuccessfully attempting to use these capabilities

z/OS Security Server RACF, https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.2.0/com.ibm.zos.v2r2.icha700/icha700_Logging_and_reporting.htm

Conclusion

Most organizations claim that their most important security issue is around data protection. The DS8000 family of storage systems is designed to meet the most demanding data protection and security requirements of the enterprise. In this paper we have discussed some of the most recent and most important technologies for security and data protection. These technologies include Logical Corruption Protection, encryption of data at rest, considerations for using host based encryption, z/OS security for protecting advanced functions from misuse, multi-tenancy features such as Resource Groups, and other important features. Users are encouraged to use the references provided within to get a deeper understanding and how-to instruction how to implement.