DELL EMC DATA DOMAIN
SECURE MULTI-TENANCY

A Solution Brief for implementing Replication as a Service (RaaS)

ABSTRACT
As cloud delivery of data protection services such as BaaS, DRaaS and RaaS are maturing, Enterprises and Service Providers (SPs) are looking to deliver cloud based data protection services in both private and public clouds to improve top and bottom line revenues. With this, the ability to create strict separation between user data so that one customer does not have access to another customer’s data along with simplified management is becoming increasingly important for delivering innovative business services with a low TCO that are cloud ready. Today, the lack of native support in enterprise data protection products for such capabilities is inhibiting the adoption and rapid delivery of cloud ready data protection services by both Enterprises and Service Providers. Dell EMC with Data Domain’s secure multi-tenancy (SMT) is providing an effective cloud ready solution that addresses these challenges.

August, 2017
# Table of Contents

**EXECUTIVE SUMMARY** .................................................................................................................. 3

**THE CHALLENGE** ............................................................................................................................ 3

**SOLUTION OVERVIEW** ...................................................................................................................... 3

**INTRODUCTION** ................................................................................................................................. 3

**AUDIENCE** ........................................................................................................................................ 3

**BACKGROUND** .................................................................................................................................. 3

  **LOCAL BACKUP SERVICES** ............................................................................................................... 4

  **REPLICATED BACKUP SERVICES** ................................................................................................. 4

  **REMOTE BACKUP SERVICES** .......................................................................................................... 4

**DATA DOMAIN SECURE MULTI-TENANCY (SMT) OVERVIEW** ......................................................... 4

**SMT SOLUTION FOR RAAS** ............................................................................................................... 5

  **SIZING** ........................................................................................................................................... 6

  **RECOMMENDED REPLICATION TYPES FOR DIFFERENT USE CASES** ......................................... 6

  **SECURE MULTI-TENANCY WITH RAAS** ....................................................................................... 8

  **REPLICATION TYPES FOR SP CONSIDERATION** ......................................................................... 8

    **Managed File Replication (MFR)** .............................................................................................. 8

    **MTree Replication (MREPL)** ................................................................................................... 9

  **SP DEPLOYS REPPLICATION USING MREPL (MTREE REPLICATION)** ........................................... 9

  **SP DEPLOYS REPPLICATION USING MFR (MANAGED FILE REPLICATION)** ............................... 11

  **MANAGEMENT, REPORTING AND CHARGEBACK** ...................................................................... 13

  **REPLICATION LIMITS/QUOTAS (FOR MTREE REPLICATION)** .................................................... 14

  **MREPL REPLICA CAPACITY QUOTA BEST PRACTICE** ................................................................ 14

  **CONFIGURING REPLICATION FOR RAAS** ................................................................................... 16

  **NETWORKING CONSIDERATIONS** ............................................................................................... 17

**BENEFITS OF DATA DOMAIN SECURE MULTI-TENANCY** ............................................................... 19

**CONCLUSION** .................................................................................................................................... 20

**ADDITIONAL RESOURCES** .............................................................................................................. 20
EXECUTIVE SUMMARY
Delivering cloud ready protection services such as BaaS, DRaaS and RaaS with multi-tenancy is increasingly adopted by both Enterprises for their internal IT and by Service Providers for delivering innovative business services. Today, Enterprises and Service Providers are using Data Domain’s Secure Multi-Tenancy (“SMT”) to deliver cloud based data protection services in both private and public clouds to improve top and bottom line revenues.

THE CHALLENGE
As cloud-based delivery of protection services such as BaaS (Backup as a Service), DRaaS (Disaster Recovery as a Service) and RaaS (Replication as a Service) are gaining traction with Service Providers and Enterprises, many are looking to address three main issues when delivering services to their customers.

Cost reduction – How do I reduce my costs both in terms of operating costs but also CAPEX with better utilization and simpler management?

Flexibility – Should I keep or replace my backup application; keep or eliminate tape infrastructure; self-managed or fully managed service … customers want the ability to choose the options that best fit their situation.

Cloud-like capabilities - Multi-tenancy, elasticity, self-service access, metering for chargeback, etc.

SOLUTION OVERVIEW
Dell EMC® Data Domain is providing an effective multi-tenant strategy to address the challenges faced by Service Providers and Enterprises in delivering cloud based protection services to their customers. This paper discusses Dell EMC Data Domain’s multi-tenant solution for RaaS that a Service Provider or an Enterprise can quickly and easily implement.

INTRODUCTION
The purpose of this white paper is to provide important technical information on designing, configuring and deploying RaaS by Service Providers and Enterprises.

SPs delivering cloud-based data protection services are gaining momentum by using technology solutions that enable scalable shared or leveraged multi-tenant infrastructures, multiple services for data protection, and the ability to meet or exceed service level agreements across a wide range of tenant needs. By delivering cloud-based data protection services, SPs can “operationalize” backup services and the costs associated with servers, software, tape libraries, tape, offsite transportation, storage and IT personnel. By leveraging new and industry leading technologies, SPs are delivering cost-effective data protection services to their customers, while reducing the requirement for upfront capital expenditures and dedicated personnel. This enables greater focus on their core business IT needs.

AUDIENCE
This white paper is intended for SP technical IT staff looking to better understand and implement RaaS using Dell EMC Data Domain. It describes how Service Providers can leverage Dell EMC Data Domain’s secure multi-tenancy capabilities to build effective cloud-based data protection services. It includes key technical considerations and factors for deployment in multi-tenant environments. It is also important that the SP has detailed understanding of the Data Domain system’s secure multi-tenancy features and key concepts. Please refer to the Data Domain System Administration Manual for details.

BACKGROUND
While we will generally describe the primary use cases in this section for which Service Providers can leverage Dell EMC Data Domain’s secure multi-tenancy to deploy data protection as a service in a public, private or hybrid cloud, the focus for this paper is RaaS (Replication as a Service).
LOCAL BACKUP SERVICES
For a large enterprise, this means hosting a local backup for multiple business units or departments. For a service provider, this means they are hosting the customer applications as well as data protection and need to logically isolate customer’s data onsite. This is defined as providing data protection services for physical or virtual servers that are located within the data center of the SP. These servers may be provided by the SP in a Compute as a Service (CaaS) or Infrastructure as a Service (IaaS) model, or could be tenant-owned servers located in the data center in a co-location agreement.

REPLICATED BACKUP SERVICES
For a large enterprise, this is likely to protect multiple remote sites that have a small local Data Domain system and each one replicates into the main data center. For a service provider, this is what we refer to as ‘DR as a Service’ – where the customer has a local Data Domain system onsite, and replicates to the service provider site – usually because they do not have their own DR facility. Here a SP could be providing a replication target for customers who own their own backup application and/or Data Domain infrastructure and have a desire or requirement to offsite a second copy of their data. The Replicated Backup Services delivered as RaaS is the focus of this white paper.

REMOTE BACKUP SERVICES
For a large enterprise, this is most likely protecting multiple remote offices that do not leverage local backup so they backup over the WAN to a Data Domain system at the main data center. In a service provider environment, this would be Backup as a Service, where customers backup from their sites over the WAN to the service provider’s facility.

DATA DOMAIN SECURE MULTI-TENANCY (SMT) OVERVIEW
With Data Domain secure multi-tenancy (SMT), a Data Domain system can isolate and securely store the backups and replication data for multiple tenants. Each tenant has logically secure and isolated data and control paths on the Data Domain system.

MTree(s) and DD Boost storage unit(s) are allocated to each tenant to store their data.

Tenant units are a fundamental unit of a multi-tenancy organization on a Data Domain system. One or more tenant units are created for each tenant, and each tenant’s MTree(s) and DD Boost storage unit(s) are then assigned to the tenant’s tenant unit(s).

![Figure 1: SMT Overview](image)
Note:

- While there is no logical limit to the total number of tenant units per Data Domain system, you do not want to configure more tenant units than the number of MTrees supported on the Data Domain system because it doesn’t make sense to have a tenant unit without any MTrees.

- You can have a tenant span multiple Data Domain systems.

Data access to each MTree is restricted to the owning tenant by configuring the protocol (DD Boost, CIFS, NFS, Replication, etc.) used to access each MTree.

Tenant administrative access to tenant units and the MTrees, which each tenant unit contains, is restricted by assigning management users or groups (AD or NIS) roles on the tenant’s tenant units, and then providing the appropriate user credentials to each tenant.

In Data Domain terminology, pre-comp is the logical capacity i.e. data written before compression while post-comp is the storage used after compression. Pre-comp written is the total amount of data sent to the MTree by backup servers. Pre-compressed data on an MTree is what a backup server sees as the total uncompressed data held by an MTree-as-storage-unit. Logical capacity (pre-comp) quotas on tenant MTrees can be configured to enforce capacity SLAs.

When using the DD Boost protocol, soft and hard quotas can also be configured on the number and types of streams (read, write, replication, and total) allowed per storage unit (for hard quota, only total number).

When using MTree Replication, a stream count limit can be specified for each replication context.

Historical space and performance data on MTrees and storage units within each tenant unit is collected and available through DDMC Usage Reports, and the CLI, as input to billing applications.

In addition to tenant units, tenant objects can also be created on Data Domain systems. Tenant objects are a hierarchical object on top of tenant units which are used to group the tenant units belonging to tenant together. For example, the tenant object tenA can be created to group together Company A’s tenant units tuA-1, tuA-2, and tuA-3. Likewise, tenant object tenB can be created to group together Company B’s tenant units tuB-1, tuB-2 and tuB-3. The same tenant object can be created on multiple Data Domain systems to track all of the resources (tenant units, MTrees, etc.) used by a tenant across multiple Data Domain systems. Tenant objects are also used to enforce that data can only replicated, or fast copied, from and to MTrees that belong to the same tenant.

For additional information on secure multi-tenancy for Data Domain systems please refer to the *WHY SECURE MULTI-TENANCY WITH DATA DOMAIN SYSTEMS* white paper.

### SMT SOLUTION FOR RAAS

Consider a SP scenario where the SP is delivering RaaS to their customers. In this scenario, multiple customers with backup data on their local Data Domain systems are replicating to the central SP data center site, as illustrated in Figure 2 and explained in more detail throughout the rest of this paper. Data Domain Management Center (DDMC) and CLIs are used to configure and monitor the solution for chargeback and reporting. In the rest of this white paper we will discuss the technologies involved and best practices that should be considered in configuring the RaaS solution.

Note: This paper only covers implementation of RaaS using Data Domain system capabilities and does not take into account any of the needs or requirements of any specific backup application which may be writing to a Data Domain system.
SIZING

Sizing the Data Domain system to service multiple tenants with RaaS involves evaluating the main variables that impact the choice of an SMT Data Domain system model. These are streams, number of MTrees, and total capacity. The choice of the Data Domain system model will be impacted by all, since it is possible that a customer’s capacity requirement is too large to fit on a candidate SMT Data Domain system, or that a customer would have so many replication contexts that they could consume all the streams of a candidate SMT Data Domain system. At the same time a customer with too many MTrees could max out the Data Domain system even if they didn’t use all the space available.

- **Capacity**
  - When onboarding a new customer, consider the maximum projected capacities of all the existing customers including the new customer on the Data Domain system to decide if the system has enough capacity for the projected time frame. Additionally, from an operational cost perspective, you will want to decide if it would be better to have multiple smaller Data Domain systems to split the projected customer capacities or have larger Data Domain systems that could host more.

- **Streams**
  - Since the number of streams on the SP target Data Domain system will be split between replication and any other process that the SP is offering (tape-out, recovery etc.) to correctly size the streams requirement, you need to evaluate the number of streams each tenant would use at any given time.
    - Number of streams used per replication context, when using MTree replication.
      - What are the maximum streams that each replication context will use based on the source Data Domain system model?
      - Calculate the maximum streams that a tenant will concurrently use by adding up the maximum streams that can be used by concurrently running replication contexts. This could max out the number of contexts/streams available on the target Data Domain system even if there is sufficient space capacity available on the target Data Domain system for the tenant.
      - The network bandwidth/speed available will impact how fast a replication context will release streams.
    - The CLI command “system show performance” on the Data Domain system shows a historical record of how many replication streams were used by the Data Domain system.

- Each Data Domain system can support a maximum number of MTrees. That limitation could be reached by customers using multiple MTrees. For example, many customers with multiple MTrees can fill the Data Domain system even if they do not use all the space or streams available.

- Other considerations are how many network cards, Fiber Channel cards would be installed into each Data Domain system. Since adding cards in a Data Domain system requires a service interruption, you need to correctly configure the Data Domain system right from the start.

**RECOMMENDED REPLICATION TYPES FOR DIFFERENT USE CASES**

With the many-to-one replication topology illustrated in Figure 2, hundreds of remote customer sites can be protected by one SP site.

- Any Data Domain system model can be the source
- Destination capacity on the SP Data Domain system should be sized to accommodate data from all remote sites
- Cross-site de-duplication results in optimal network usage

Figure 3 shows the recommended replication types for different use cases.
<table>
<thead>
<tr>
<th>Use case</th>
<th>Recommend replication type</th>
</tr>
</thead>
<tbody>
<tr>
<td>When using dedicated Data Domain systems for protecting production Data Domain system</td>
<td>Collection replication</td>
</tr>
<tr>
<td>When using applications with DD Boost integration</td>
<td>Managed File replication</td>
</tr>
<tr>
<td>When using MTrees for logically partitioning a Data Domain system</td>
<td>MTree replication</td>
</tr>
<tr>
<td>When replicating user-created snapshots to destination Data Domain system</td>
<td>MTree replication</td>
</tr>
<tr>
<td>When using Data Domain systems with Data Domain Extended Retention license</td>
<td>MTree replication</td>
</tr>
<tr>
<td>When using archive data sets</td>
<td>MTree replication</td>
</tr>
<tr>
<td>When using compliance or governance archive data locked with Data Domain Retention Lock</td>
<td>MTree replication</td>
</tr>
</tbody>
</table>

The replication algorithm is resilient and capable of dealing with different WAN conditions. As illustrated in Figure 4, the replication protocol delivers:

- Automated optimization for parallel transfer (per MTree/per Data Domain system VTL pool) of files
  - One stream per file modified/closed within the interval
- Results in higher throughput; thereby lowering the RPO
- Counters effect of latency and packet loss
- System-controlled behavior – user intervention not required

![Figure 3: RaaS deployment – Replication choices based on use cases](image)

![Figure 4: RaaS deployment – Replication choices based on use cases](image)
SECURE MULTI-TENANCY WITH RAAS

With RaaS, the Data Domain system at the source is replicating to tenant units on the central Data Domain system at the destination (SP data center site). Each tenant unit at the destination provides security and isolation at the replication target. This is the typical Cloud deployment, where the tenants are customers of Replication as a Service provided by the SP through Data Domain system’s SMT.

An MTree is said to belong to a tenant object if the MTree is contained in a tenant unit that belongs to that tenant object.

SMT security and isolation ensures that if the source MTree belongs to a tenant and the destination MTree belongs to a tenant then replication is only permitted if the source and destination tenants are the same. This rule applies no matter what security-modes are configured on the tenant units (see below) that contain the MTrees.

SMT provides two security-modes for varying security level requirements and varied deployment scenarios. The security-modes are – strict and default.

If strict security-mode is configured at either the source or destination tenant unit, then both the source and destination tenant units must belong to a tenant (because of the earlier isolation rule, this obviously must be the same tenant), in order for replication to be allowed between MTrees in the source and destination tenant units. Note that because a SP typically does not have control over the tenant Data Domain system, we recommend that security-mode strict generally should not be configured on the SP’s destination tenant units.

The default tenant unit security-mode permits replication to or from the MTrees in the tenant unit, from or to MTrees that do or do not belong to a tenant. However as always, if both the source and destination MTrees belong to a tenant, replication is only allowed if both MTrees belong to the same tenant.

Encryption over the wire should be configured to protect customer information during the replication.

REPLICATION TYPES FOR SP CONSIDERATION

While there are multiple different replication types for addressing different use cases (see Figure 3), in the context of the SP delivering RaaS, we will consider and discuss MTree Replication (MREPL) and Managed File Replication (MFR) types. In the following sections we will examine the best practices involved when deploying these replication types in a SP environment.

MANAGED FILE REPLICATION (MFR)

You want to use MFR when using DD Boost protocol with your backup application. The advantages of MFR include:

- Fully controlled by the backup application (through DD Boost) and optimized by Data Domain systems
- Single interface for backup policy management
- With DD Replicator, Data Domain system sends only unique data
- Maintain different retention policies for each file
- Keep de-duplicated remote copies for longer duration
- Recovery from primary or replicated copies
- Tracks and reports when a backup image (files) is completely replicated
- File replication takes place after a backup image is completed
- Supported topologies: one-to-one, bi-directional, many-to-one, one-to-many
MTREE REPLICATION (MREPL)

You want to use MREPL when replicating user created snapshots to the destination and/or when using other, non-DD Boost protocols such as NFS, CIFS, VTL etc. The advantages of MREPL include:

- Replicates NFS, CIFS, and VTL data
- Contents of entire MTtree replicated to the destination
- Destination MTtree is read-only
- Leverages snapshots of source MTtree
- Sends periodic updates
- Destination is always a point-in-time image of source
- Snapshot created on source MTtree is automatically replicated to the destination. Note: SP can leverage the user created snapshot management capability to create and maintain user snapshots to protect tenant data from a scenario where accidental data operations (deletes/overwrites) on the source get replicated to the destination and they lose the previous good data on destination too. In this scenario, SP could offer an optional service to create a user snapshot every x-weeks and preserve the last N such copies for recovery purposes.
- No need to create snapshots separately on source and destination for point-in-time recovery
- Retention period of user-created snapshot replicated to destination
- Flexible replication topologies
- One-to-one, bi-directional, one-to-many, many-to-one, cascaded

SP DEPLOYS REPLICATION USING MREPL (MTREE REPLICATION)

Customer backup data will be stored in MTrees and can be used with Data Domain systems using the 3 supported protocols; NFS Shares, CIFS Shares and VTL.

Scenario 1 – Network bandwidth can support direct seeding to the SP site

In this scenario, data can be replicated directly to the SP site.
Pro:
- No need to modify the customer backup environment
- Only need Data Domain system to Data Domain system connection
- Normal deployment method for NFS/CIFS/VTL based backups

Con:
- Backup software is not aware of secondary images on the destination/target Data Domain system at SP site
- Will need to import the images back into customer backup software before using them for tape out or recovery
- Requires more steps to recover the images from the SP site for the customer

Scenario 2 – Network bandwidth cannot support direct seeding to the SP site

In this scenario, data cannot be replicated directly to the SP site and will need local seeding at customer/tenant site using a seeder Data Domain system.

Step1: Seed the data from source Data Domain system onto the seeder Data Domain system using MREPL. Create a user snapshot on the Mtree, and wait for it to be visible on the Seeder.

Step2: Break replication to Seeder and ship Seeder to SP site.

Step3: Start seeding from the seeder Data Domain system (now at the SP site) to the destination Data Domain system (at SP site) using MREPL. Wait for the seeding from the Seeder Data Domain system to destination Data Domain system to finish (the user snapshot should be visible on the destination Data Domain Mtree).

Step4: Resync MREPL from source to destination. Delete the user created snapshot from the Mtree on the source Data Domain system.

Pro:
- No modification needed on customer backup software
- Same approach can be used for any type of backup

Figure 6: Indirect seeding to SP site using MREPL
Con:

- Backup software is not aware of the secondary images on the destination/target Data Domain system at the SP site
- Will need to import the secondary images back into customer backup software before using them for tape out or recovery

**Important Note:** There was a bug reported against the above seeding procedure (Bug ID# 138888) in DD OS 5.5.1.0. The seeding procedure described above cannot be used unless the source, seeder, and destination Data Domain systems are running DD OS versions with the bug fixed (5.5.3.0 or later).

Please call into Dell EMC Data Domain support for the correct DD OS version that resolved the aforementioned bug.

**SP DEPLOYS REPLICATION USING MFR (MANAGED FILE REPLICATION)**

Customer backup data will be stored in Storage units and can be used with Data Domain using DD Boost protocol. Backup software will use Managed File Replication (MFR) to a target Data Domain system at a secondary site at SP. The advantages are that backup software is aware of the secondary images on the target Data Domain system and the images can be recovered from the secondary Data Domain system. We have 3 options to replicate the backup images to the destination SP Data Domain system.

**Scenario 1 – Use MFR to replicate directly from customer to SP site**

Using the backup software with DD Boost, use MFR to replicate the customer/tenant source Data Domain system data to the SP destination Data Domain system directly.

![Diagram](image)

*Figure 7: Direct seeding to the SP site using MFR and DD Boost*

**Pro:**

- Backup software is aware of secondary images at SP site
- Easy for the customer to use secondary images at SP site
- Can be used for tape out
- Can be used for recovery from the SP site directly (DRaaS)

Note: Some verification will be needed in order to recover images from the secondary Data Domain system (bandwidth, latency)
Con:

- Need knowledge of backup software operation
- Need to modify customer backup environment
- Require connectivity from backup server to the SP Data Domain system

Scenario 2 – Use MREPL to seed to local Data Domain system (seeder) and then recreate DD Boost structure using MFR once seeding is done

In order to reduce the impact and modification to the customer environment the following solution can be used.

- Create MPEPL from customer’s DD Boost Storage unit to the seeder Data Domain system. Once they are in sync, ship the seeder Data Domain system to SP location.
- Re-establish replication and then create cascading replication from the seeder Data Domain system to the SP’s shared Data Domain system.
- Once everything is in sync, the SP shared Data Domain system will have all the blocks from the customer’s storage unit.
- You can then create the cloning/replication (MFR) in the backup software from the customer’s production Data Domain system to the SP’s shared Data Domain system. This will recreate the storage unit structure without having to resend the data.

Pro:

- No modification on customer backup software for the seeding

Con:

- Backup software is not aware of images at SP until MFR is accomplished

Figure 8: Indirect seeding to SP site using MREPL and MFR
MANAGEMENT, REPORTING AND CHARGEBACK

We recommend that the SP use Data Domain Management Center to configure and manage SMT on their Data Domain system. DD Management Center provides SMT configuration wizards, and tenant/tenant unit level views of storage (MTrees, Storage units) and replication for easy monitoring and troubleshooting. DD Management Center also provides reports and graphs containing historical and current space and performance usage at the MTree, tenant unit, and tenant levels. Usage metrics can be exported via Excel spreadsheets for import into SP billing programs.

SP also has the option to use CLIs if they choose to do so. Please refer to the DDMC user guide and DD OS administrative guide respectively for additional information.

SP can use the physical capacity measurement (PCM) features of DD OS 5.7 for chargeback reporting based on physical capacity consumed by each customer’s data. Below are two CLI screen shots showing PCM output for two Secure Multi-tenancy objects, one for tenant t1 and another for tenant unit tu1. The DDMC usage report provides similar tenant, tenant-unit, and MTree logical and physical capacity measurements in an Excel spreadsheet, which might be more convenient for import into chargeback/billing programs.

For details on PCM reporting, please refer to the Data Domain Physical Capacity Measurement white paper.
REPLICATION LIMITS/QUOTAS (FOR MTREE REPLICATION)

Stream limits per MTree replication context

MTree Replication with SMT allows for setting both stream limits per replication context, and capacity quotas on both the source and destination Data Domain system systems. The SP can set upper limits on the streams on a per replication context basis that is enforced on the Data Domain system where it is set up (source or destination). For example if the customer sets a streams upper limit of 32 (Note that there is a 32 max system stream limit per MTree replication context) for a given replication context at the source Data Domain system that is local to their site and the SP sets a streams upper limit of 20 for the same replication context on the destination Data Domain system in their data center, the MTree replication will proceed using the lower of the stream limits set at source (customer site) and destination (SP data center site) for the replication context (per the checkboxes in the below figure). This allows the SP to control and throttle data from different customers so a single mis-behaving customer cannot overload the shared, Data Domain system at the SP site. See figure 9 below.

![MTree Replication Diagram]

Figure 9: Stream limits per replication context

Capacity quota on MTree Replication (MREPL) replica

The Service Provider (SP) owning the destination Data Domain system can set capacity quotas on the replication destination MTree to limit tenant capacity usage. In DD OS 5.7, as part of SMT features, the user is allowed to set a capacity quota on the MREPL destination MTree. This allows the SP/Tenant to be notified when replica capacity quota is breached, and then take appropriate action.

MREPL REPLICA CAPACITY QUOTA BEST PRACTICE

In DD OS 5.7, as part of SMT requirements, the Data Domain system administrator is allowed to set capacity quotas on MREPL destination MTrees. This allows the SP/Tenant to be notified when replica capacity quota is breached, and then take appropriate action. The following acronyms are used in this document:

RHCQ – Replica Hard Logical Capacity Quota

RSCQ – Replica Soft Logical Capacity Quota

Note: MTree quotas apply only to the logical data written to the MTree. An administrator can set storage space restrictions for an MTree, storage unit, or VTL pool to prevent it from consuming excess space. There are two kinds of quota limits: hard limits and soft limits. You can set either a soft or hard limit or both a soft and hard limit. Both values must be integers, and the soft value must be less than the hard value. When a soft limit is set, an alert is sent when the MTree size exceeds the limit, but data can still be written to it. When a hard limit is set, data cannot be written to the
MTree when the hard limit is reached. Therefore, all write operations fail until data is deleted from the MTree. As the SP, you have to decide whether to configure hard or soft limits on the logical capacity for your tenant’s MTrees and whether to notify them of quota breaches. We recommend that you set soft limits so tenant operations are not failed. Please refer to the Data Domain Administration Guide documentation for details.

General guideline for using RHCQ and RSCQ in SMT environment

- RSCQ can be set appropriately to proactively manage the capacity on the replica.
- Use RHCQ only when it’s absolutely necessary. There are serious and unintended consequences when RHCQ is breached.
- If RHCQ is set, RSCQ MUST be set to a desirable value in order to get an early indication that RHCQ is about to be breached and proactive actions must be quickly taken.

When should Replica Soft Capacity Quota (RSCQ) be used?

It is a good practice to set RSCQ in the SMT environment. It allows the SP to manage and forecast the capacity usage of the tenants, and take proactive measures when the RSCQ is breached.

- The USQC value must be low enough that the SP can respond in time to avoid a hard quota breach (if set) or out of space on the replica.
- SP should allocate sufficient capacity on replica to allow temporary over-subscription.

When should Replica Hard Capacity Quote (RHCQ) be used?

RHCQ is used only if the SP MUST prevent specific tenants from constantly over-subscribing the capacity on the replica, thus affecting SP’s business operations. Alternatively, RSCQ can be set, instead of RHCQ, so when it is breached, the SP can manually disable replication for this particular tenant to prevent disruption to the SP business. If RHCQ is breached or if there is no more free space on the replica, replication will stop making progress. When this happens, the tenant’s DR SLA can quickly be violated. The longer this condition persists, the longer it will take for replication to catch up. If this condition persists for too long, replication may never be able to catch up, and the tenant data will need to be reseeded on the SP Data Domain system. Therefore, the SP/tenant must be proactive to avoid this situation.

- RHCQ is preferred over RHCQ because proactive action taken when RSCQ is breached can prevent interruption in replication.
- If a RHCQ is set on a destination MTree, then a RSCQ MUST also be set. The SP should establish guidelines on what value to set for the RSCQ. For example, the RSCQ could be set to the capacity contracted with the tenant for that MTree, and then the RSHQ set 25% higher than the RSCQ. In any case the RSCQ value must be low enough that the SP can respond in time to avoid a hard quota breach.

When RSCQ is breached, both the tenant and the SP will receive a capacity soft quota breached alert. Replication will continue. If the RSCQ is set to the capacity contracted with the tenant, this serves notice to the tenant that their contracted capacity limit has been breached, and that the SP is not required to supply additional capacity to the tenant. This should prompt the tenant to ask the SP for more capacity or reduce their usage.

Recommended action

1. If sufficient space is available and with agreement with Tenant to pay for more capacity, the SP should increase the RSCQ and RSHQ.
2. Disable replication. Provider and tenant have the option to favor ingest over replication and disable replication if they don’t want to consume network until the quota issue is resolved.
When RHCQ is breached or when there is no more free space on the replica

SP and tenant will both receive a capacity hard quota capacity breached alert (via email).

Replication is interrupted until the issue is resolved.

Recommended action

1. If sufficient space is available and with agreement with Tenant, SP should permanently increase RHCQ and its corresponding RSCQ. Replication should recover automatically.

2. If RHCQ is reached on the replica and there is sufficient replica space available, but the tenant does not want to increase their contracted capacity, the SP can temporarily remove RHCQ or increase the RHCQ on the destination MTree. This will allow the tenant to continue replicating while they delete data in the source MTree in order to conform to their contracted capacity. It is not required to immediately run filesystem clean after deleting logical capacity. The next scheduled run of filesystem clean will reclaim the freed space. SP can re-enable or set RHCQ to previous value once situation is under control.

3. The SP should ensure that the network and Data Domain system resources allocated to the tenant are sufficient to enable tenant replication to catch up after an outage that lasts as long as the time it takes the SP to resolve this condition.

4. If the tenant does not want to, or the SP cannot increase RHCQ, the tenant should break replication, remove enough data on the source to get under the RHCQ (delete and run filesystem clean), and then resync the replication. Note: Replication resync must start with a snapshot that is under RHCQ. Therefore, snapshots that are over the RHCQ must be removed before resyncing. MTree size must be checked against RHCQ before starting resync.

5. If there is a replica space issue or SP cannot increase the RHCQ because of replica space issue, the SP must make room on the destination Data Domain system by removing or migrating some other data from the destination Data Domain system. Another option is that the SP must migrate the tenant to another Data Domain system with enough capacity.

6. If a long delay is likely before replication can be successful, either the tenant or the SP can disable replication to avoid consuming Data Domain system and network resources.

CONFIGURING REPLICATION FOR RAAS

To setup the Data Domain to Data Domain system pairing from the customer’s source Data Domain system to the SP target Data Domain system, here are the steps involved:

MTree and collection replications can be configured by running the appropriate CLI commands on each Data Domain system. This doesn’t require either the source or destination administrator to know the sysadmin credentials of the other Data Domain system. For example, to set up an MTree replication (in the example below, the /data/col1/m3 MTree must already exist), ask the tenant/customer to run the below CLI commands on the source Data Domain system at their site:

```
replication add source mtree://dd120-20.datadomain.com/data/col1/m3 destination mtree://dd160-9.datadomain.com/data/col1/m103
```

or

```
replication add source mtree://dd120-20.datadomain.com/data/col1/m3 destination mtree://dd160-9.datadomain.com/data/col1/m103 encryption enabled if encryption is required.
```

Then run exactly the same CLI commands on the destination Data Domain system owned by the SP in this case (/data/col1/m103 must NOT already exist on the destination – it will be created by the replication when it is initialized):

```
replication add source mtree://dd120-20.datadomain.com/data/col1/m3 destination mtree://dd160-9.datadomain.com/data/col1/m103
```

or add encryption enabled (if encryption was configured on the source)
Then, back on the source Data Domain system, ask the tenant to run the following command to initialize (start) the replication:

```bash
replication initialize mtree://dd160-9.datadomain.com/data/col1/m103
```

You should see messages as below indicating that the replication is starting.

(00:09) Waiting for initialize to start...

(00:11) Initialize started.

The full set of CLI commands that are used to set up and configure replication are documented in the *Data Domain OS Command Reference Guide*.

**NETWORKING CONSIDERATIONS**

The Data Domain system is a dual stack system and supports both IPv4 and IPv6. Therefore whatever address the hostname is resolved to, whether it is IPv4 or IPv6, that address will be used to replicate. Since the base network has been IPv4, the support for IPv4 cannot be turned off on the Data Domain system i.e. IPv4 is always enabled, it can’t be turned off. On the other hand the IPv6 networking can be disabled on the Data Domain system.

As illustrated in Figure 10, the replication protocol supports replication over both IPv4 and IPv6 WANs with the below capabilities:

- Collection replication, and MTree replication can replicate over IPv4 and/or IPv6 networks
- Managed File Replication (for DD Boost) supports IPv6 networks
- A Data Domain system can replicate over both IPv4 and IPv6 addresses
  - Both replication contexts must be of same address family

Figure 10 shows the Data Domain systems working in the dual environment as well as IPv4 only and IPv6 only.

![Figure 10: Encrypted Replication](image)

**Network Topology considerations**

It is important to note that Data Domain system does not directly support overlapping IP ranges. If this condition exists, alternate networking techniques (e.g.: 1:1 NAT, NAT Overload / PAT, etc.) external to Data Domain system must be used to separate the duplicate address ranges.
Consider a sample network topology where the customer is replicating to the SP Data Domain system. When going over the public internet, for additional security you might want to use an encrypted tunnel (beyond Data Domain’s in-flight encryption). It is important to note that you can configure the replication pairing by pointing the customer Data Domain system to the public address of the SP Data Domain system NAT IP address.

![Network Topology](image)

Whatever the network topology, the key to enable successful replication pairing is for the customer’s source Data Domain system to know the destination IP address of the Data Domain system in the central SP data center.

**Connectivity from customer to SP**

SP should consider offering different types of connectivity from the external customer/tenant sites to the SP. The SP Data Domain system target can be configured with a management “FQDN” ip that faces the SP environment and get access to the network services; ntp, dns, smtp, snmp, reporting/management. This connection is internal and will not be used or seen by the customer. For better network separation for administrative purposes, SP should configure specific customer/tenant IP address to specific IP address on the SP’s destination Data Domain system. Such Local-IP and Remote-IP pairing when specified for a tenant unit, provides authentication for self-service administration that is restricted based on these IPs. The SP should provide the customer with a questionnaire to setup a permanent VPN. Once the VPN is active the customer can now connect to the Data Domain system and proceed with the replication. The other option is to provide direct connectivity from the customer to the SP site. They can then go through the LACP or configure a direct connection to the Data Domain system.

**Other networking considerations**

In a LAN environment there can be multiple logical LANs on the same physical LAN. These can be separated by using multiple subnets on the same LAN. Therefore the Data Domain systems will use different interfaces based on what subnet is being used. This isolation can further be controlled by using VLAN tagging with each VLAN having a different subnet. The VLANs can be exposed to the Data Domain systems by using trunked switch ports or they can be hidden from the network end points by configuring the switch ports as access point. Of course it is not necessarily all or none. There can be some switch ports that are configured as access points and some configured as trunks with the Data Domain systems providing its own VLAN checking with multiple VLANs on one interface, each with its own subnet. If a switch port supports multiple VLANs it is better to have it configured as a trunk and let the end point keep the VLANs separated. The Data Domain system does this and it works well with DD Boost using ifgroups (now called Dynamic Interface Groups).

In the WAN environment it can get complicated. In a LAN environment it usually works with non-routable addresses (i.e. private IP addresses not routable across the public Internet) which are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16. There is usually enough to handle any LAN environment and since they are non-routable they are confined to the specific LAN and other LANs can have the same IP address. An example of this is mall, private networks. These networks use the address range of 192.168.1.0/24. This does not conflict with other home networks because when a packet from the home network gets routed out of the LAN onto the WAN it is given another address that is global which is referred to as a NAT (Network Address Translation), but in the mall, private network case it is usually PAT (Port Address Translation) where the same global address is used for multiple address translation and the TCP port number is used to differentiate...
between the different LAN addresses. Therefore even less global addresses are needed but if there is a server on the LAN that is needed to be connected from the outside there will need to be a NAT not a PAT. If there is a Data Domain system inside the LAN then then a NAT will need to be used to connect to it.

This is further complicated if the tenant/source Data Domain system is on a different LAN and also has a NAT being done. This would be referred to as a double NAT. The tenant/source Data Domain system will only know the Data Domain system’s public address and the Data Domain system will only know the tenant/source Data Domain system’s public address. This can be further complicated by the need for the tenant/source Data Domain system to look like it is on the same subnet and even the same VLAN as the Data Domain system. Normally the global address from the Tenant/Source Data Domain system side would just be passed through the NAT on the Data Domain side, but in this case the address would be modified using a process called masquerading to look like it is on the same subnet as the interface on the Data Domain system. Figure 11 demonstrates this.

One would think that with IPv6 addressing the NAT is no longer needed with the massive number of address available, but the NAT also provide a level of security and also flexibility to allow multiple servers to provide the same service to multiple Tenant/Source Data Domain systems. The NAT architecture will continue with the IPv6 addressing.

One other complication with the WAN architecture is the use of VPN. This activity is done independently and transparently to the Data Domain system and therefore does not impact the connection. That is, the Data Domain system does not have to do anything special or different when a VPN is used. On the other hand when NAT is done it will impact the address that is used. The Tenant/Source Data Domain system cannot tell the Data Domain system what address it is using because it only knows the private address not the public address. The DNS on the Data Domain system LAN will need to map the Tenant/Source Data Domain system’s FQDN to the public addresses (or the masqueraded address), not the private addresses, but it will have to map the Data Domain system’s FQDN to the private address for Tenant/Source Data Domain systems on the same private LAN as the Data Domain system. A similar thing must be done on the Tenant/Source Data Domain system side.

Networking summary – Putting it all together

The SP needs to consider different types of connectivity to and from external customer/tenant sites to the SP. The Data Domain system may be configured with a management FQDN and a data FQDN which both gets translated to an address and the remote Tenant/Source Data Domain system would have the FQDNs translated to a public accessible IP addresses. There will be a need to have access to local services like DNS, SMTP, ntp, snmp, but some will need to provide similar data to the Tenant/Source Data Domain system side. For example, the time from ntp needs to match on both sides but the DNS needs to have the mappings that allow the systems to get the addresses necessary to connect to the remote system. Each tenant should be on different VLANs with different subnets. The Data Domain system local addresses need to be paired to the Tenant/Source Data Domain system unique address which will give the restricted access necessary for each tenant. Note there may be multiple Tenant/Source Data Domain systems and Data Domain addresses for each tenant. These also may be configured into ifgroups to allow DD Boost to provide this isolation between tenants. If desired, VPNs can be setup but these will be transparent to the Data Domain system. It will usually be transparent to the Tenant/Source Data Domain system too. Encryption can also be used which is available with the replication.

**BENEFITS OF DATA DOMAIN SECURE MULTI-TENANCY**

Secure multi-tenancy for Data Domain can dramatically improve protection storage efficiencies for large Enterprises and Service Providers.

Secure multi-tenancy will help Enterprises & Service Providers:

- Achieve secure data isolation by tenant on shared Data Domain systems.
- Reduce data protection storage costs.
- Shorten time for service requests.
- Enable efficient IT as a Service for Data Domain protection storage.
• Provide tenant self-service administration and reporting.
• Efficiently manage Data Domain system streams and capacity.
• Simplify Data Domain system capacity planning.
• Give the provider control over capacity and stream count resources assigned to each tenant on shared Data Domain systems.
• Deliver Protection Storage as a Service and/or Replication as a Service in private cloud environment and for service providers in a hybrid or public cloud environment.

CONCLUSION
This paper has stated that cloud delivery of data protection services such as BaaS, DRaaS and RaaS are maturing and has provided details and best practices on how a Service Provider or an Enterprise IT can efficiently implement a RaaS solution in a public, private or hybrid cloud, using Dell EMC Data Domain secure multi-tenancy’s cloud ready capabilities. Dell EMC Data Domain’s secure multi-tenancy gives Service Providers and Enterprises flexibility in delivering innovative data protection services to best meet their scalability & accessibility needs and can be leveraged with any existing backup software that may already be deployed in the data center.

ADDITIONAL RESOURCES
Dell EMC Data Domain Physical Capacity Measurement – Solution Brief – Technical white paper
Dell EMC Why Secure Multi-tenancy with Data Domain Systems – Business Value paper
Dell EMC Data Domain Replicator – Lightboard Video
Data Domain DD OS 5.7 Secure multi-tenancy – Narrated Demo
Data Domain DD OS 5.7 Physical capacity measurement – Narrated Demo
Data Domain Boost and Dynamic Interface Groups - Solution Brief – Technical white paper
Data Domain Data Invulnerability Architecture – Technical white paper
Why Data Domain – Business Value paper