Abstract
This white paper describes how Service Providers can leverage EMC Avamar to build effective cloud-based data protection services. It includes key technical considerations and factors for deployment in multi-tenant environments.

March 2012
Copyright © 2012 EMC Corporation. All Rights Reserved.

EMC believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

The information in this publication is provided “as is.” EMC Corporation 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 EMC software described in this publication requires an applicable software license.

For the most up-to-date listing of EMC product names, see EMC Corporation Trademarks on EMC.com.

VMware is a registered trademark of VMware, Inc. in the United States and/or other jurisdictions. All other trademarks used herein are the property of their respective owners.

Part Number H10584
# Table of Contents

**Executive summary** ........................................................................................................... 5  
Audience .................................................................................................................................. 5  

**EMC’s Next Generation Data Protection Solution** ................................................................. 6  

**Deployment models** ............................................................................................................ 7  

**Avamar architecture** ......................................................................................................... 8  
The Avamar agent .................................................................................................................. 8  
Avamar Data Store Hardware Architecture ............................................................................. 10  
Single-Node Avamar Data Store System ............................................................................. 11  
Multi-Node Avamar Data Store System ............................................................................. 11  
RAID ..................................................................................................................................... 12  
RAIN ..................................................................................................................................... 12  
Replication ............................................................................................................................. 12  

**Networking architecture** .................................................................................................... 13  
Secure network access ......................................................................................................... 14  
Virtual LAN (VLAN) Tagging ............................................................................................... 15  
Network Address Translation (NAT) ..................................................................................... 15  
Networks & deployment models ............................................................................................ 17  

**Sizing your Avamar environment** ....................................................................................... 17  
Size of the data set & retention periods .............................................................................. 18  
Simultaneous connections .................................................................................................... 19  
Recovery Time Objective / Recovery Point Objective (RTO/RPO) ....................................... 19  
More discussion about data types ....................................................................................... 20  
Unstructured data ................................................................................................................... 21  
Structured data ...................................................................................................................... 22  

**System security** .................................................................................................................. 22  
Authentication / administration ............................................................................................ 22  
Avamar domains .................................................................................................................... 23  
Avamar roles-based users ..................................................................................................... 23  
Administrator roles .............................................................................................................. 24  
Operator roles ....................................................................................................................... 24  
User roles .............................................................................................................................. 25  
Client/Server authentication ................................................................................................... 25  
Data encryption ...................................................................................................................... 26  
In-Flight encryption ............................................................................................................. 26  
Stunneling .............................................................................................................................. 26  
At-Rest encryption ............................................................................................................... 26  

**Reporting** ........................................................................................................................... 27
Avamar standard reporting ........................................................................................................ 27
EMC Data Protection Advisor (DPA) Integration ....................................................................... 28
Management Console Command Line Interface (MCCLI) ............................................................. 29
Support ..................................................................................................................................... 29
Conclusion ................................................................................................................................. 29
Links to additional information ................................................................................................. 30
Executive summary

Over the last five years, the Service Provider (SP) market has gained a great deal of momentum. Enterprises of all sizes are increasingly procuring IT in “As a Service” (aaS) solutions. The need for rapid deployment, reduced total cost of ownership, and overall agility are fueling this shift. Backup as a Service, Disaster Recovery as a Service along with other data protection as a Service offerings are exploding onto the scene enabling new revenue streams for SPs and unparalleled solutions and flexibility for consuming Enterprises.

Delivery of cloud-based services via shared/leveraged infrastructures has gained significant mindshare with enterprises, as they seek to solve data protection challenges caused by increasing volumes of data, shrinking backup windows, fewer IT personnel and 24x7 business operations. Today’s data protection solutions must protect diverse enterprise environments with various applications, data types and workloads on virtual as well as physical infrastructures residing in data centers, remote offices, and desktop/laptop systems. At the same time, they face stringent service levels, and the need to reduce costs and maximize available resources.

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.

EMC’s efficient solutions enable SPs to deliver data protection services to even broader markets. The integration of Data Domain deduplication storage systems into Avamar provides additional flexibility in development of the most efficient data protection solution possible. These tightly integrated solutions enable the SP community to build unsurpassed services that enable more efficient solutions for their customers and greater revenue streams for the SP’s at unsurpassed SLAs.

Audience

This white paper is intended for SP technical IT staff. It describes how Service Providers can leverage EMC Avamar 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 understand the inner workings of the solution including communication protocols, security, reporting and integration. These topics are covered in other technical documents - please refer to the document links at the end of this paper.
EMC’s Next Generation Data Protection Solution

EMC Avamar backup and recovery software and systems provide fast, efficient backup and recovery for VMware® environments, LAN/NAS systems, remote offices, desktops/laptops, and enterprise applications. By deduplicating the data before it is transferred across the network (LAN, WAN, NIC), Avamar delivers daily FULL backups in a fraction of the time when compared to traditional backup applications, which typically provide only weekly fulls/daily incremendals, while transferring and storing lots of redundant data. Avamar also deduplicates backup data globally across physical and virtual servers, desktops, laptops and offices. As a result, Avamar reduces the total required storage by up to 50x, and network traffic (LAN, WAN or NIC) by up to 99% daily. And Avamar backups can be quickly recovered in just one step - eliminating the hassle of restoring the last good full and subsequent incremental backups to reach the desired recovery point. In addition, data can be encrypted in flight and at rest for added security.

This enables industry leading backup, recovery, and disaster recovery via existing IP LAN/WAN links - all of which dramatically lower the SP’s capital and operating expenses, including floor space, power and cooling. As the SP environment grows, monitoring multiple Avamar systems is easy via the Avamar Enterprise Manager. This intuitive interface provides the SP with a dashboard view that shows the status of each system at a glance, providing data such as capacity utilization, system alerts and job status. And SP Administrators can drill down into individual systems as needed, simplifying management for local or remote Avamar systems. These operational benefits contribute to the delivery of cost-effective SP services.

Avamar 6.0 includes the ability to direct and manage backups simultaneously to Avamar Data Store servers and Data Domain deduplication storage systems. All management is performed via the Avamar Administration Console, allowing quick and easy direction of enterprise-wide backups to either storage platform based on data types and characteristics. This integration provides the SP with the benefits of the Avamar application’s simplicity, the efficiency of the Avamar Data Store and the increased scale and performance of Data Domain systems.
In a cloud-based SP delivery model, it is important to understand the benefits that each storage subsystem can deliver to the environment, and design the solution using one or both of these options based on the data protection needs. This allows the most efficient and cost-effective solution to be enabled for SPs and their customers. Some SP solutions may be best served utilizing Avamar Data Store servers, while others may benefit most from Data Domain systems, but in many cases a combination of the two will provide the best solution and the most flexibility. The single interface allows the SP to easily manage the solution from a single pane of glass, which reduces the overall complexity, management, and IT costs.

Deployment models

We are discussing various technical considerations for the three deployment models that were covered in the “EMC Avamar – Business Deployment Considerations for Service Providers” paper:

• Local Backup Services: 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.

• Remote Backup Services: Avamar backup infrastructure is located within the SP data center, and is accessed with backup via agents that are installed onto the production servers physically located on the customer’s premises.
• Replicated Backup Services: providing a replication target for customers who own their own Avamar and/or Data Domain infrastructure and have a desire to offsite a second copy of their data.

In these three deployment models, the biggest drivers are centered on networking and the various requirements driven by the proximity of the primary data and the backup infrastructure, coupled with enablement of those networks connections in a multi-tenant environment. We will focus on these areas, as well as other areas of keen interest such as the roles-based security model and interfacing/reporting options that can be used within the Avamar solution.

Avamar architecture

Avamar is a complete enterprise backup and recovery solution designed around client/server architecture. The Avamar software agent is deployed on the client systems being protected and communicates over a TCP-IP network with the Avamar Data Store or Data Domain deduplication storage system where the data from the clients is collected and stored. The Avamar software application runs on each Data Store node, performing all of the data protection management operations such as scheduling backups, setting retention periods and managing data recovery processes. This client/server architecture communicating over TCP-IP forms the basis for many of the multi-tenant deployment drivers within the solution.

It is important to understand the how the Avamar system functions as we look at considerations for system sizing and network/interconnection setup. This will allow assurance that the systems can meet the defined SLAs for the offering and drive optimum cost reductions across the entire SP functional organization.

The Avamar agent

The Avamar agents are the cornerstones of the Avamar enterprise backup and recovery solution. The functionality provided by the Avamar agent goes well beyond that found in traditional backup software agents, enabling data deduplication at the client before data is sent across the physical or virtual infrastructure (network, WAN and storage).

Upon executing a backup, the Avamar agent scans the file system looking for new or changed data from the previous backup. A small cache of file metadata is
maintained at each client server, allowing the Avamar agent to compare the current file metadata to the file metadata logged during the previous backup, and determine if a file is new or has changed. It is only necessary to process new or changed files.

When a new or changed file is identified, the Avamar agent uses a patented process to create unique sub-file variable length data segments that are 1 byte – 44 KB each. The Avamar agent leverages another small cache file stored on the client server that tracks the data segments that have been encountered during previous local backup jobs. The Avamar agent checks this data segment cache to determine if it has been seen in a previous backup job on this server. If the sub-file segment is in the local cache then it is known to have existed during a previous backup and therefore can be skipped. This greatly reduces the “chattiness” on the network when performing global deduplication across sites and servers. If the segment is not in the local cache, the Avamar agent contacts the Avamar Data Store server to see if that unique segment is already stored in the global segment storage pool. If the data segment exists on the Avamar Data Store, this signifies that the segment has already been encountered and backed up during another job, so it is not transferred again.
added to the local data segment cache file to make all subsequent backups more efficient. It is the two processes discussed above, global data deduplication (only storing one copy of each sub-file data segment regardless of how many times it exists in the enterprise) and deduplication at the client that enables fast, daily full backups via existing IP networks, significantly reduced network traffic, and a reduction in backend disk storage of up to 50x.

The main connectivity consideration for the Avamar agent is that it must have the ability to resolve the IP addresses for all nodes in the Avamar Data Store system, either by use of DNS entries or via host file entries on each server. This will be discussed more in a later section of this paper.

**Avamar Data Store Hardware Architecture**

The Avamar Data Store is an all-in-one packaged solution consisting of EMC Avamar software running on preconfigured EMC-certified hardware. It is available in two models – a scalable multi-node model and a single-node model. This approach simplifies purchasing, deployment, and service while minimizing on-site setup.

The multi-node Avamar Data Store is designed for the data center where backup data is being consolidated from multiple remote locations or to protect VMware environments and LAN/NAS servers. It can efficiently retain the equivalent of up to several petabytes of traditional cumulative daily full backups.

The single-node Avamar Data Store is ideal for deployment at remote offices that require faster local recovery. A variety of single-node capacities are available, which under a typical traditional backup schedule could require hundreds of terabytes of disk or tape storage, depending on the backup method and retention period. In addition, both multi-node and single-node models support replication, either from the remote office to the data center for consolidation, or between data centers for disaster recovery. These deployment options provide for varying levels of data resiliency, coupling high availability options like RAID, RAIN and Replication to ensure effective system protection.

The Avamar Data Store systems include two components:

- **Utility Node**
- **Data Nodes (Active and Spare)**

Single-node Data Store systems combine the Utility Node and Data Node functionality into a single server. In these single-node systems, only basic features for fault tolerance (i.e.: RAID and dual power supplies) are provided. Multi-node Data Stores have the combined advantage of high availability features and increased backup/recovery performance. Each of these nodes will be assigned an IP address and FQDN for external connections from the Avamar agents.
Single-Node Avamar Data Store System

A single-node Avamar Data Store provides the functionality of both the Utility Node and the Data Node. It is designed to meet the needs of smaller offices, which may not need a multi-node system or for those users with RTO SLAs that cannot be met via backup/recovery over existing wide area network lines. Single-node systems can be deployed as physical hardware or as a virtual systems running under VMWare.

The EMC Avamar Virtual Edition for VMware is the industry’s leading deduplication virtual appliance for backup, recovery, and disaster recovery. It enables an Avamar server to be deployed easily, effectively, and in a repeatable fashion on VMware ESX Server hosts, leveraging the existing server CPU, memory, and disk storage.

It is important to note that since this is a single-node system, RAIN is not used. These single-node systems should be replicated to another Avamar system (single- or multi-node) to provide effective protection against a failure of the single-node system. Backup and replication processes can be comingled on a single NIC port or separated out on different NIC ports as desired.

Multi-Node Avamar Data Store System

An Avamar multi-node Data Store system is comprised of a single utility node for system administration and multiple data nodes for storage of backup data objects.

The Utility node is the access point to the Avamar Management Console for setting up backup policies, including definition of datasets, backup schedules and retention policies. The utility node is the driver for all scheduled backup jobs. As scheduled backup windows come around, the utility node will create a detailed work order for each backup agent in the scheduled group. The work order is then sent to the corresponding Avamar agent (if the agent is “pageable” — more on that topic in the NAT section) running on the production server, with the agent then taking over the backup process. It is important to note that once the utility node sends the work order, it is no longer in the active backup “loop” until the backup job completes. The utility node does receive periodic updates (20-30 second intervals) from the agent to update the status of the job in the Activities window.

At the end of the backup, the agent will send the wrap-up data to the utility node signaling the completion and final status of the backup job, with this status logged in the Management Console database. It is critical to understand how this process works and how different network architectures can impact how these functions flow. These will be discussed in the networking section of this paper.

In a multi-node Avamar Data Store system, 3 to 16 active data nodes can be configured for storage of backup sub-file data segments. Systems can be initially sized with a smaller number of data nodes (3 minimum), and then expanded to the maximum 16 data nodes supported in a multi-node grid. This capability to scale up is delivered by the patented Redundant Array of Independent Nodes (RAIN) architecture discussed later in this paper. There may also be a spare data node on each grid that can be used in the event of a complete data node failure to rebuild the data objects, again leveraging RAIN.
Data Nodes are specifically designed to balance CPU, memory, data storage capacity and I/O throughput. The ratio of CPU power, memory, throughput and capacity are designed to scale almost linearly. This allows optimal system performance for backup, replication as well as a number of post-backup maintenance operations as the system grows. The system is designed this way in order to provide the best overall RAS (reliability, availability, and scalability).

**RAID**

Every Avamar Data Store node in every configuration leverages RAID for data availability. This provides the ability to withstand the failure of a drive in the node without rendering the node inoperable. These drives are hot-swappable to provide the minimal impact during drive replacement.

**RAIN**

Redundant Array of Independent Nodes (RAIN) is a patented Avamar technology that enables parity data to be striped across the active data nodes in the Avamar Data Store multi-node systems. This ensures that each data node in the system can be rebuilt using this parity data in a similar process as that used by RAID-5 parity striping across drives. By striping parity data across drives and data nodes in the system, the Avamar Data Store achieves a much higher degree of reliability and fault tolerance.

RAIN is also responsible for providing the ability to add data nodes to an Avamar multi-node system. As a system grows to capacity, additional data nodes (up to a maximum of 16 active data nodes) can be added to the system to increase data object storage. When adding new data nodes to the system, a rebalance command is issued. This causes the Avamar system to rebalance the storage of the data objects across the data nodes in a linear fashion, ensuring that there is generally equal utilization of storage on each data node, and therefore delivering scalable backup and recovery performance as the system grows.

In many cases, solutions become slower as they grow larger. With Avamar, overall performance increases as the system gets larger. The spare data node may also be used as a stop-gap measure when a system begins to fill to capacity, giving the ability to start the add/rebalance process quickly while new data nodes are procured. If the spare data node has been added to an active configuration, a new spare node should be acquired promptly and made available to the Avamar Data Store system.

RAIN, like RAID has overhead. It is important to note that, just like RAID-5, the fewer number of data nodes in a RAIN system configuration, the greater the effective overhead. When configuring an Avamar multi-node system, the EMC Backup System Sizer will take this RAIN overhead into account and size appropriately.

**Replication**

Replication is an additional level of availability designed into the Avamar system. Data can be logically replicated from a source Avamar system to a target Avamar system. It is important to note that if you are using both Data Store and Data Domain
for storage and you plan to replicate the data, you must replicate both storage infrastructures.

Replication uses the same deduplication technology to move backup data segments between the client and target Avamar systems. This allows the SP a great deal of flexibility in designing configurations for customers to deliver automated movement of data off-site as either a standard part of the service or as a value-added service.

Replication only transfers the net new backup data segments. Moving data off site over an IP network becomes a viable option with deduplication technologies combined with the declining costs of bandwidth. These new technologies offer a reduction in bandwidth utilization and security features that enable better data protection solutions with less greatly reduced risk for “lost” data.

The replication process is initiated by the utility node on the source Avamar system and the concept is similar to a backup job performed from the source utility node to the target Avamar system. Any new data that has been added to the source system since the last replication job will be logically replicated to the target system. The utility node will walk through all of the backup datasets for all clients (in alphabetical order) on the source system looking for new data. This deduplication process is the same as that outlined in the section on the Avamar agent backup flow, using “is-present” calls to the target Avamar system to ensure global deduplication. It is also possible to modify the replication data retention policies during replication.

Replication from the source utility node is configured to use the same NIC port as is used for backups. If separation of backup traffic and replication traffic is desired, outbound replication from the source Avamar system can be configured to use an alternate NIC port. Connectivity from the selected NIC must have the ability to communicate/resolve ALL nodes (utility and all active data nodes) at the target Avamar system.

Networking architecture

Earlier in this document, we talked about how Avamar is an Enterprise Data Protection solution built upon a client / server architecture that communicates over TCP-IP networks for Agent-to-Data Store and Data Store-to-Data Store interactions. As we have discussed, each Avamar node will have an IP address and FQDN assigned for identification. The Avamar agent must be able to resolve all of these node addresses within the system (single- or multi-node) to which they are activated.

When operating in a multi-tenant environment, there are several customers that are accessing the Avamar infrastructure, and in most cases from dedicated, non-shared “private” networks. This means that a single NIC port on each node must be used for connection to the “backup” network across all of these customers. This requires a number of different factors be taken into account when setting up each individual Avamar system (single- or multi-node) to service these multiple tenants. Each of the different deployment models will also potentially represent different challenges that
may require some standard networking techniques to overcome to allow maintaining this private network separation but also allow the sharing of the Avamar system.

This section is meant to outline how Avamar can be setup to support deployment in various scenarios requiring different networking processes. We will not go into the details around how to configure specific external networking devices to make each configuration work, as this is beyond the scope of this document. Instead we will highlight the processes and standards that should be leveraged on these devices and how Avamar interacts. The detailed setup and operation of these network devices is the responsibility of the SP.

**Secure network access**

When architecting an Avamar solution, the Avamar system must reside in a secure data center behind a firewall and be accessed securely from remote sites. It is important that the communication between the client devices and the Avamar server are as secure as possible. EMC does not support installation of the Avamar system on the open Internet.

It is not technologically impossible to have an Avamar system configured with public IP addresses and sit on the Internet, but because of the nature of the client/server architecture and the need for communications to all nodes in the Avamar grid, this opens up different means by which unscrupulous attackers can try to compromise the system. To alleviate this concern, EMC requires that these systems sit inside a secure network that is effectively firewalled from the public Internet to minimize intrusion attempts. If access from remote sites is required, we recommend the SP setup a secure connection via VPN (either connection-based or point-to-point) or other secure networking methodology.

If using VPNs, deployment can be done in a few different ways; 1) Point-To-Point VPN Tunnel or, 2) VPN SW agents. If using point-to-point persistent tunnels between hardware devices located at the customer site and the SP data center, the secure connection is always “on”, and therefore does not need to be established at the start of each backup job. If a VPN SW solution is to be used, then a process must be created that will setup the VPN connection from the remote server running the Avamar agent into a VPN concentrator at the SP data center. This connection could be done using a manual user process, but is not very flexible or robust when trying to create
an automated data protection scheme. If using a SW VPN, the best plan would be to use a backup pre-script at each server that would setup the VPN connection automatically, run the backup job, and then stop the VPN with a backup post-script. When setting up the Avamar datasets, these pre- and post-scripts will be designated to run before and after the Avamar backup process. The specifics format and method of calling these scripts will vary based on the VPN solution. The downside to using this method is the requirement to create a custom script for use at each server where the agent is installed.

One other potential option that could be used to strengthen network security is MAC Address Filtering (MAF) at the SP data center. A MAC address is unique hardware address that is burned into each network interface device installed in a computer. Some think MAF is for wireless network access only, but it can be applied to physical network devices as well as long as the routing device supports it. MAF adds another layer of checks into the process of connecting into the SP network. With MAF, the router maintains a list of the unique MAC addresses that are authorized to communicate with the SP network. TCP-IP packets received with MAC addresses on the list are allowed to pass into the network. MAC addresses that do not match are discarded. This can be a very effective layer of security added to the inbound networking plan, but it does require additional effort to setup and manage. Whenever a new Avamar agent is setup on a new device, that new device’s MAC address would need to be added to the router list. It is important to note that MAF alone is not “bullet-proof” as there are some methods the determined hackers can use for spoofing MAC addresses.

**Virtual LAN (VLAN) Tagging**

The Avamar system (GEN4 HW or greater) can be configured to support the 802.1Q networking standard for VLANs. This gives the ability to create multiple virtual network channels (via VLAN Tags) into a single NIC port on each node within the Avamar system. Avamar supports VLAN tags in the range of 1-4094, giving the system the ability to support multiple “private” networks on the single NIC. VLAN tagging gives the Avamar system the ability to have a different virtual IP address for each VLAN, and therefore ease routing constraints. The specific VLAN configuration is setup/modified within each Avamar node using an Avamar utility called “dpnnetutil”, and is covered in the Avamar technical note “Configuring VLAN Traffic Over Different Subnetworks”.

It is important to note that Avamar does not directly support VLANs that have overlapping IP ranges. If this condition exists, alternate networking techniques (e.g.: 1:1 NAT, NAT Overload / PAT, etc) external to Avamar must be used to separate the duplicate address ranges. It is also important to note that Avamar also does not support separate DNS servers on each VLAN.

**Network Address Translation (NAT)**

In most customer environments, IP addressing schemes are based private non-routable IP ranges (e.g.: 192.X.X.X, 10.X.X.X) devised for use within their internal
environment. When we start to look at the need to route information to an external location, we must now look at how we can best enable that communication to take place. When we look across these private networks, there is relatively high probability for overlapping IP addresses. NAT is an address translation scheme that can allow IP address ranges to be modified on either a one-to-one basis (1:1 NAT), or to utilize a single IP address to enable multiple clients to communicate externally (NAT Overload w/Port Address Translation). Using one or more of these translation schemes, the SP can adapt to or maintain a structure of unique addressing to support these different customer networks. NAT routing rules are “managed” external to the Avamar system, but Avamar provides all of the things needed to support this within the backup application given our unique needs.

When using client side NAT (Avamar side NAT is not supported, as there would then be no way for connections to be established), the addresses that the clients use to communicate with the Avamar nodes are going to be different than the “real” IP addresses for each node. In order to support this process, the Avamar system uses a configuration file on each node that provides the translation of the real IP addresses for each node with the corresponding NAT’ed address for each customer private network. The Avamar system can be configured to simultaneously support non-NAT customers as well as multiple NAT ranges for multiple customer private networks.

It is important to note that when using NAT Overloading, some Avamar functionality is rendered unavailable. Specifically, this relates to functions requiring client paging and client browsing. These functions require the Avamar utility node be able to initiate communications with the Avamar agent running on each client. NAT Overloading effectively masks the actual end user IP address, therefore the Avamar Management Console has to wait for the Avamar agent’s periodic “check-in” to initiate connection back to the utility node thus allowing any open work order for that agent to be sent. This means that scheduled backups and recovery requests may be delayed by as much as the time delay set for the periodic check-in process.

EMC recommends that when operating in a configuration where NAT is being used, the default check-in delay should be changed from 60 minutes to 5-15 minutes. You must balance check-in delay to overall system performance; having hundreds of Avamar agents checking in every minute could have a negative impact to the overall system performance because it is spending so much time processing check-in
requests, yet on the other hand having a check-in of 60 minutes means that scheduled agent processes could be delayed by as much as 59 minutes in a worst case scenario. In general, we find that in smaller environments (1-100 agents), a 5-minute check-in period can be supported. 100-300 clients should increase to 10 minutes, and then 15 minutes for all other from 300-600.

**Networks & deployment models**

In general, we have found that support for the networking schemes discussed above will provide the SP with the needed flexibility to deploy in almost any customer environment. Many times, a hybrid approach of various network schemes is needed, all of which can be supported simultaneously within the Avamar solution.

**Sizing your Avamar environment**

Sizing the Avamar Data Store system for Service Providers requires an understanding of how the system protects and manages information. There are a number of factors that determine the Avamar Data Store configuration. Factors that influence the Avamar Data Store size are:

- The type of data in your environment
  - Unstructured: File System (generally very good deduplication rates due to the repetitive nature of data across productivity type files)
  - Structured: Database/Email/PSTs (generally lower deduplication rates due to unique nature of the data)
  - Movies, Music, Mother Nature (M3) (Although these are unstructured data files, data within each file is VERY unique and does not deduplicate well across files.)
  - Compressed data: Compressed data has a lower deduplication rate due to the way various compression algorithms work. If possible, it is best to backup uncompressed data to maintain the best deduplication rates.
  - Encrypted data: Encrypted data files have poor deduplication rates. This is due to the fact that as the data is modified, by design the encryption product will save it with a new encryption key making all of the data within the file look different. It is best to ensure that you are backing up unencrypted data, otherwise Avamar storage utilization will be VERY high.

- The amount of data for each data type
- The retention period of each data set
- The number of agents connecting into the Data Store
- The customer’s SLA for RPO / RTO

It is understood that within an SP environment, there may not always be insight to the exact mix of data that will be protected within a given Avamar system. There is no
deduplication process that will provide the same levels of high deduplication across all data types; some data types just deduplicate better than others. As you are building out the business plan, it is critical that you look at the market that you plan to target, and start to make some assumptions around the mix of data types that you think you will see in those environments. Will it be mostly unstructured data, structured data or some mix of the two? Are you targeting a market segment that may have larger amounts of data types that deduplicate poorly like music and video files? This is the kind of data that will be critical to understand while you are sizing the underlying Avamar infrastructure and developing the costing models.

It is also critical to understand that although the Avamar system is very scalable, there is going to be periods of performance degradation when you add new nodes to the system. In the SP environment, it is not wise to try and size the base system for an individual customer, then add nodes based on the needs of each individual new customer you add to the service. Each add-node process will have an SLA impact to ALL of the customers being serviced by the multi-tenant Avamar grid. You COULD do it this way, but based on our experience with various SPs, it is not advised. The better approach is to install a larger infrastructure that will accommodate the growth that you anticipate for the first 12-18 months of the service. This would mean installing the complete hardware infrastructure up front, then “trueing-up” software licensing on a periodic basis (monthly/quarterly). This approach would benefit from higher ingest performance, higher restore performance and lower RAIN overhead, yet delaying the Avamar software licensing cost until it is actually being used. In many cases, the most successful SPs have developed a plan of installing the largest system (16 active data nodes) such that they then never have to worry about the node-add process at all. They get the benefit of the additional backup and restore performance delivered by the maximum node configuration right from the inception of the services.

As we size the Avamar system, we will use all of these data assumptions to build the baseline system required, from which you will be able to build the service cost model.

**Size of the data set & retention periods**

The configuration of the Avamar Data Store can be calculated by taking the volume expected from all customers, identifying the breakdown by data type (making some assumptions on the data’s change rate) and combining this information with the standard retention policies the SP plans to offer. This information is then entered into the EMC Backup System Sizing tool to determine the minimum number of data nodes required in the Avamar system to support those data volumes with those assumptions. As discussed earlier, it is recommended to configure and install sufficient capacity to provide for at least 1.5 years of planned deployments and growth in the service.
Simultaneous connections

Another component to take into consideration when sizing a Data Store is the number of simultaneous users that would need to connect into the Data Store for backups.

With Avamar version 6.0, each Avamar data node in an Avamar system can support 17 simultaneous backup and recovery processes. A single-node system uses 16 channels for backup or recovery, always leaving one channel open for recovery. For example, in a 10 data node system, there are 170 channels available, 169 for backups or recovery and 1 for recovery. This single connection is maintained to ensure that the Data Store can always perform recoveries, even while the system is backing up. When backups are not running, the system can be directed to utilize one channel from each data node for a single recovery operation.

When configuring an Avamar system, each node also contributes to overall system throughput. Therefore you should not only look at capacity requirements but also throughput requirements for backup ingestion and data restoration. A properly architected Data Store will yield a positive result for all your SLAs. In all but the most demanding environments, the Data Store nodes are never the bottleneck.

It is also important to note that today there is a limitation of the number of users and groups (domains) that can be assigned to one Avamar Data Store. A single-node Data Store can manage a maximum of 500 domains and 1,000 agents. A multi-node Data Store can manage a maximum of 1,500 domains and 5,000 agents. These limitations are not a function of the Data Store itself but more of a function of the User Interface (UI) of the system and how the system can be effectively managed. Work is being done to expand this number, but EMC rarely sees these levels as a limiting factor.

Recovery Time Objective / Recovery Point Objective (RTO/RPO)

One of the key differences that exist in the SP environment is the whole process of delivery to an SLA. The SP must define the SLA that is included as part of the service, and then be able to measurably perform to that SLA. The most important SLA issue with backup over the WAN is not only backing up the data within the required window
but also the recovery of the data within the defined Recovery Time Objective (RTO). As customers plan their SP backup strategy, they need to define and plan for a “worst case scenario” recovery event to be covered by the RTO. Two important factors to consider when planning for recovering data over the WAN: 1) bandwidth between the service provider and the user and 2) the amount of data to be recovered.

Users need to identify their RTO in order to ensure they can successfully meet their objectives for data recovery. If the amount of data required for recovery cannot be pushed over the given network infrastructure between the customer and the SP to meet the RTO, then putting a local Avamar Data Store on the customer’s premises would be required. Customers would backup to a local Avamar system and replicate the data to the Avamar system managed by the SP. Avamar technology is an excellent fit for this scenario. As previously discussed, Avamar utilizes the same data deduplication algorithms used for backup are also used for replication.

By backing up locally and replicating, customers can take advantage of two levels of protection while meeting their RTOs. Additionally, the Avamar team has tools that can help identify, based on a data volume and bandwidth, whether or not a customer will need a local appliance or not.

**More discussion about data types**

From a client perspective, the most important factor that contributes to the efficiency of the Avamar system is the change rate on the client. Windows file systems that contain a great deal of personal productivity application data (Word, Excel, PPT, PDF) have very low change rates and can be propagated throughout an enterprise. Hence, there is a high degree of commonality not only in a file system but also across the enterprise as these files are often emailed to others.

Linux and Unix file systems tend to have less commonality. These file systems usually have specific application data of varying types and this data does not typically move as prolifically throughout the enterprise.

![Type of Data](image)

Structured data environments such as databases or email applications tend to have a higher degree of change. Data sets with a higher degree of change take longer to
back up and require more storage as a function of this change. This concept is true not only for data deduplication solutions but first generation backup technologies as well. If you think about how IT generally protects databases, they traditionally do full backups every night. Due the nature of the change rate in a database, the delta between an incremental backup and a full is not a large difference. Additionally, since the recovery of structured data tends to have faster recovery time objectives (RTOs), performing a single step recovery can lead to faster RTOs.

As discussed above, data types typically break down into two categories, structured and unstructured data types. Unstructured data takes the form of Word, Excel and PowerPoint files. Structured data takes the form of database data such as SQL and Oracle as well as Email data such as Exchange. Each of these data types has very different characteristics. The biggest difference in these data types is primarily around their rate of change. Data with higher change rates will cause more unique data objects to be created and therefore require more movement and storage of that unique data during backups.

**Unstructured data**

Personal productivity applications that typically fall into the Windows OS environment such as Word, Excel, PowerPoint, etc makes up a very large component of the unstructured data set. Unstructured data typically has a very low change rate and produces a high degree of common, duplicate not only across systems but locally on a single system as well.

For example, if you take a look at a person’s work system or a file share in an office, there tend to be a lot of files that have much common information among them. For example, PowerPoint presentations are copied over and over again in order to maintain copies for specific purposes, with different users adding slides for different events. Not only is the content in these presentations the same, each slide has the same “master slide” content producing an even higher degree of commonality. MS Word documents from a contracts department contain a great deal of similar information. The executive summary may be different across contracts as the point of the contract may have different context, but the pricing information, support information, training information etc., is all the same. The same phenomenon exists with MS Excel files. As the Avamar client agent scans through each file system it only needs to move one copy of the content, no matter where it exists, into the Avamar server for the entire environment to reference. In a typical customer’s environment, as much as 80% of their data falls into this unstructured data type.

On initial backups of unstructured data, customers typically see 30 to 70 percent commonality across multiple systems. The data deduplication efficiency grows as more systems are protected. As more systems are backed up to the Avamar Data Store, less data is moved to the Data Store, even on an initial backup. The day over day commonality is between 99.3% and 99.7%.
Structured data

Structured data includes databases such as Oracle, DB2 or SQL. It may also be in the form of semi-structured data such as Email systems like Exchange or Notes, or file share systems such as SharePoint. Some specific file types, like Exchange PST files, also exhibit characteristics of structured data. Key factors to keep in mind:

- Size of the data set
- Change rate of the data

The larger the size of the structured data set and the higher the change rate, the longer it takes for a client based deduplication application to process the data and move it to the Avamar Data Store.

Traditional backup applications track changed data by reviewing a file’s date and time stamp. As files change, the date and time stamp will be different. This is an indication to move or backup the file. A second generation, client based deduplication application tracks the files that have changed and then applies an algorithm to the changed file to find only the blocks (variable or fixed) with the file that have changed. The time required for this deduplication processing is directly related to the size of the dataset. Service providers need to take these facts into consideration when helping their customers architect a data protection solution.

System security

One of the most important factors when deciding to utilize a service provider is security. The security of data in transit and at the service provider site can be the biggest obstacle when it comes to trusting a service provider. This is why there are a number of security features in the Avamar solution:

- Authentication – User Names / Passwords
- Avamar Domains – logical segregation of customers
- Avamar Roles-based Users - who has the ability to perform certain tasks in the Avamar Data Store
- Client/Server Authentication
- Data Encryption – In flight and at rest

For more information, please refer to the EMC Avamar 6.0 Product Security Guide available on EMC PowerLink.

Authentication / administration

The Avamar authentication system is a username/password system that is used to grant users access to the Avamar server. Avamar supports its own internal authentication system, as well as several external authentication systems such as Network Information Service (NIS), Open Lightweight Directory Access Protocol
(OpenLDAP), and Windows Active Directory. The choice of authentication can be provisioned through the Avamar Administration Console.

In the Avamar system, user accounts can be added to domains or individual clients. When you add a user account to a domain, the account can administer that domain and any subdomains beneath it. When you add a user account to an individual client, the account can perform backups and restores of that client, and access backups belonging to that client in the system. Avamar user accounts comprise the following pieces of information:

- Username
- Authentication system
- Role

Roles define various allowable operations for each user account. There are three basic categories of roles:

- Administrator roles
- Operator roles
- User roles

**Avamar domains**

Avamar domains are distinct zones within the Avamar server that are used to organize and segregate clients. This provides enhanced security by allowing administrative user accounts to be defined on a domain-by-domain basis. It should be understood that Avamar domains are completely internal to the Avamar server and have nothing to do with Internet domains.

Avamar Domains can be nested to create a rich structure for segregating multiple customers in a multi-tenant system. Each customer would be setup as a subdomain under the Avamar root domain. This would provide the ability to assign specific domain roles to specific customer users for the desired level of access and features desired by the SP. It should also be understood that there is no functional difference between domains and subdomains. “Subdomain” is merely a term that refers to any domain nested within another higher-level domain.

**Avamar roles-based users**

Roles define various allowable operations for each user account. There are three basic categories of roles:

- Administrator roles
- Operator roles
- User roles

Users with these roles would leverage the Avamar Management Console for login/access into the Avamar system. The appropriate network ports would have to
be opened to allow for this management traffic to pass through from the customer site to the SP site as required.

Alternately, the SP can utilize the Management Console Command Line Interface (MCCLI) to integrate Avamar features into a custom portal to provide these types of capabilities as desired. This would require the SP to manage the access to the specific functions made available via their custom portal.

**Administrator roles**

Administrators are generally responsible for maintaining the system. The role of administrator can only be assigned to user accounts at a domain level. This role cannot be assigned to user accounts at a client level. The role of administrator can be assigned to user accounts at the top-level (root) domain, or any other domain or subdomain.

Root Administrators: Administrators at the top-level (root) domain have full control of the system. They are sometimes referred to as “root administrators.” This role would be reserved for the SP Administrators due to the fact that they would have access to all domains in the Avamar system. Root Administrators can also access the Avamar Enterprise Manager which gives an administrative dashboard view of multiple Avamar systems for monitoring purposes.

Domain Administrators: Administrators at lower level domains (other than root) generally have access to most of the Avamar administration features, but typically can only view or operate on objects (backups, policy objects, and so forth) within that domain. Any activity that might allow a domain administrator to view data outside that domain is disallowed. Therefore, access to server features of a global nature (for example, suspending or resuming scheduled operations, changing runtimes for maintenance activities, and so forth) is disallowed. Furthermore, domain administrators:

- Cannot add or edit other subdomain administrators
- Cannot change their assigned role
- Can change their password

**Operator roles**

Operator roles are generally implemented to allow certain users limited access to specific domains within the Avamar system to perform backups and restores or obtain status and run reports. These roles allow greater freedom in assigning backup, restore, and reporting tasks to persons other than administrators.

As with administrator roles, operator roles can only be assigned to user accounts at the domain level; these roles cannot be assigned to user accounts at the client level. Furthermore, to add the user account to subdomains, you must have administrator privileges on the parent domain or above. There are four operator roles:

- Restore Only Operator: Perform restores and to monitor those activities to determine when they complete and if they completed without errors.
• Back Up Only Operator: Perform backups and to monitor those activities to determine when they complete and if they completed without errors.
• Back Up/Restore Operator: Perform backups or restores and to monitor those activities to determine when they complete and if they completed without errors.
• Activity Operator: Monitor backup and restore activities and to create certain reports.

Users with an operator role (non-Admin role) do not have access to all features in Avamar Administrator. Instead, after login, they are presented with a single window from the Management Console GUI that provides access to the features that they are allowed to use.

User roles
User roles are always assigned to a user account for a specific client, and not the domain. As such, allowable operations are inherently constrained to that specific client. There are four user roles:
• Back Up Only User: Users assigned this role can initiate backups directly from the client using the avtar command line.
• Restore (Read) Only User: Users assigned this role can initiate restores directly from the client using the avtar command line or Avamar Web Services.
• Back Up/Restore User: Users assigned this role can initiate backups and restores directly from the client using the avtar command line or Avamar Web Services.
• Restore (Read) Only/Ignore File Permissions: This role is similar to the Restore (Read) Only User role except that operating system file permissions are ignored during restores, thereby effectively allowing this user to restore any file stored for that Avamar client. All Windows client user accounts should be assigned this role to ensure trouble-free restores. This role is only available when external authentication is used.

Client/Server authentication
Avamar clients and servers use Transport Layer Security (TLS) certificates and Public Key Infrastructure (PKI) for authentication and encryption of data in transit. TLS and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide secure communications on the Internet for activities such as web browsing, email, Internet faxing, instant messaging, and other data transfers. Although essentially the same, there are minor differences between SSL and TLS.

Avamar supports the X.509 v3 standard for formatting digital certificates. To sign the certificates, you can:
• Use a commercial certification authority (CA), such as Verisign.
• Generate your own root certificate and set up a private CA.
• Self-sign, although self-signing is not recommended in production environments
You can configure the Avamar environment for one-way or two-way authentication between Avamar clients and the Avamar server:

- **With one-way authentication**, the Avamar client requests authentication from the Avamar server, and the server sends the appropriate certificate to the client. The client then validates the certificate.
- **With two-way authentication**, the client requests authentication from the Avamar server, and then the Avamar server also requests authentication from the client. Client-to-server authentication can be set up in addition to server-to-client authentication to provide a stronger level of security.

One-way authentication typically provides sufficient security. However, in some cases, two-way authentication is required or preferred.

**Data encryption**

Avamar encrypts all data sent between clients and the server “in flight.” Each Avamar server can also be configured to encrypt data stored on the server “at rest.”

**In-Flight encryption**

In order to provide enhanced security during client/server data transfers, Avamar supports the following encryption methods:

- Avamar proprietary
- 128-bit Advanced Encryption Standard (AES)
- 256-bit Advanced Encryption Standard (AES)

Avamar encryption is a lightweight proprietary algorithm suitable for Avamar client to server communication over trusted networks. AES is 128/256-bit Advanced Encryption Standard encryption and should be used for any network communications where security is of great concern. The choice of encryption method can be made on a client-by-client basis via client properties, or for an entire group of clients via group properties. The data is encrypted and sent over a secure SSL connection to the Avamar Data Store.

**Stunneling**

Stunnel enables SSL communications to be grafted on to applications that otherwise do not support secure sockets. Once configured, stunnel listens on a particular port waiting for an SSL connection. The default SSL Avamar server port is 29000, but can be changed to any other unused port.

Once an SSL connection has been established on the configured port, stunnel opens an outgoing unencrypted socket connection to a specified host and port, and then relays data between the encrypted and unencrypted connections.

**At-Rest encryption**

It is important to understand the customer’s drivers around encryption at rest. Many times, they equate the need with their past processes of off-siting tapes whereby
encryption was needed to protect the data in the event that a tape is lost or misplaced during transport/storage. Within Avamar, off-siting data is done via replication over IP connections to a remote Avamar system. This data movement uses encryption for the data in-flight. Providing encryption at rest is really protecting against someone removing a physical node from an Avamar system located in the SP datacenter, and being able to use data from that node. As we look at this security scenario, we also have to look at the way that Avamar stores the data objects on the system to see what data could be used if a node were stolen from the data center.

Within the Avamar solution, backup datasets are not written in a contiguous block manner to a single data node. The storage of data objects is load-balanced across all of the data nodes, so bits and pieces of each job are stored in multiple LUNS across multiple data nodes. This alone makes using data from a single data node difficult at best, but when you also take into account the object data compression that is used, the data on the system is effectively “munged” to a point that it is rendered almost useless by itself. When looking at the big picture, if there is a concern about someone stealing data node(s) from a system, there may be bigger security issues than what can be provided by encryption at rest.

The decision to encrypt all data stored in an Avamar server is a one-time decision that is made when the server is initially deployed. When data is encrypted at-rest, all LUNS within each Data Store node has to be encrypted. The Data Store cannot encrypt data in specific domains; it must encrypt all of the data in the Data Store.

The encryption algorithm used for at-rest encryption is 128 bit Blowfish encryption. When deploying “At-Rest” encryption, the Avamar system read/write performance will be impacted. The overhead is approximately 30%, so to attain the same level of system performance as outlined in EMC literature, an encrypted system must have the data node count increased by 30%. It is important to keep this factor in mind when working with customers and helping them to achieve their SLAs.

If a customer is adamant about having their data encrypted at rest, it is recommended that a dedicated Data Store be deployed specifically for that customer. This will allow encryption at rest to be enabled for their requirements without impacting system performance/sizing for all other customers as would be the case if deploying in a multi-tenant system. This also will allow a separate costing model to be created for this single customer, and not burden all customers with this increase if not needed.

**Reporting**

**Avamar standard reporting**

Avamar report tools allow you to create, manage and run various system reports. When Avamar reports are run, the results are displayed in a separate dialog box. The report results can also be exported as a Comma-Separated Values (CSV) text file.

There are 27 standard, predefined reports provided by the Avamar system:
• Bytes Protected by Avamar Client
• Bytes Protected Total
• Client Statistics
• DPN Summary
• Activity Exceptions
• Activity Failures
• Activity Successes
• Licensed Bytes Protected by Avamar Client
• Licensed Bytes Protected Total
• Licensed Clients Statistics
• Licensed Plugins Statistics
• Plugin Client Statistics
• Plugin Statistics
• Capacity Report
• Clients with No Activities
• Clients with No Check Ins
• Clients Protected
• Clients Unprotected
• System GSAN Performance Statistics

Each of these reports can be generated using any third-party PostgreSQL-compliant ODBC database reporting tool that runs on the platform. However, you must create report templates using the Avamar schema listings found in dbviews.sql.

New reports can also be created by editing the base reports, or by using one of four Avamar templates:
• Activities: Show detailed information about system activities, such as backups, restores, backup validations, and replication.
• Clients: Show detailed information about one or more backup clients.
• Replication Activities: Similar to Activities reports, but only show information related to replication.
• Backend Capacity: Show detailed information about the amount of backend capacity consumed by one or more clients.

EMC Data Protection Advisor (DPA) Integration

Avamar is also integrated to DPA to provide rich reporting capabilities from the Avamar system. In addition to backup reporting capabilities, DPA can also be used to report on a number of specific applications, storage arrays, IP switches, file servers, database applications, VMWare infrastructure and tape libraries.

For a full list of DPA supported solutions, please refer to the DPA Compatibility matrix that is available on EMC PowerLink.
Management Console Command Line Interface (MCCLI)

The Avamar Management Console Command Line Interface (MCCLI) is a Java software application that provides command line access to over 100 Avamar Administrator features and functions covering resources for interacting with:

<table>
<thead>
<tr>
<th>Activities</th>
<th>Datasets</th>
<th>Groups</th>
<th>Schedules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agents</td>
<td>DD Properties</td>
<td>Help</td>
<td>Servers</td>
</tr>
<tr>
<td>Backups</td>
<td>Domains</td>
<td>MCS</td>
<td>Snapups</td>
</tr>
<tr>
<td>Checkpoints</td>
<td>Dumps</td>
<td>Plug-Ins</td>
<td>Users</td>
</tr>
<tr>
<td>Clients</td>
<td>Events</td>
<td>Retentions</td>
<td>Versions</td>
</tr>
</tbody>
</table>

In order to connect to the Avamar server using MCCLI, you must have:

- A valid Avamar Administrator ID and password
- Network access to an operational Avamar server

The MCCLI can be leveraged by SPs to develop custom connection methods into the Avamar system and administration utilities. This can enable the SP to integrate the desired Avamar Admin features and functions into a custom web portal to deliver a common end user experience. The shell script wrapper that invokes the MCCLI java application sets various environment arguments that are required to invoke a Java application, thereby simplifying use of the MCCLI java application and making it easier to integrate into the custom portal.

Support

Service Providers who choose Avamar solutions for their infrastructure are required to attend Avamar training. There is a course entitled Installation, Configuration and Administration that explains how to install, configure and administer an Avamar Data Store. Additionally there is a course for Administration only.

Service Provider customers who take first and second level calls from customers before engaging EMC for level 3 assistance should also plan for additional training with EMC to ensure they are proficient in troubleshooting the Avamar solution. This hands-on training would be delivered by spending two weeks in the EMC | Avamar support center learning how EMC troubleshoots Avamar issues. This is an invaluable experience and goes a long way in providing quality support for your customers.

Conclusion

The Service Provider market has gained significant momentum in the last 24 months due to new technologies that efficiently move, store and manage data. The declining
cost of network bandwidth coupled with technologies such as data deduplication bring the cost of disk-based backup on par with or often lower than tape, and end users are turning to Service Providers for help in removing tedious, expensive tasks in the data center so they can focus on more strategic activities.

This growth in data protection outsourcing is driving Service Providers to obtain the most efficient and cost effective technology on the market in an effort to maximize profits and resources. This includes the ability to efficiently move data (minimize impact on network infrastructure), efficiently store data (to optimize $/GB costs), high RAS (reliability, availability and scalability) as well as ease of deployment in an effort to reduce their operational expenditures.

EMC provides end-to-end, integrated solutions, with the scale, performance, flexibility and security that Service Providers demand. Flexible solutions can be deployed entirely at the Service Provider’s data center, or in combination with elements on the tenant’s premises. As a result, Service Providers can build a long-term, differentiated and profitable set of offerings, powered by EMC Backup and Recovery solutions.

**Links to additional information**

The following documents provide additional details on EMC Avamar and Data Domain solutions, and are available via EMC PowerLink. If you need any assistance, please contact your EMC BRS sales representative.

- White Paper: Efficient Data Protection with EMC Avamar Global Deduplication Software
- White Paper: Planning for EMC Avamar and EMC Data Domain Integration
- White Paper: EMC Avamar Integration with EMC Data Domain – A Detailed Review
- EMC Avamar 6.0 MCCLI Programmer Guide (P/N 300-011-640)
• EMC Avamar 6.0 Administration Guide (P/N 300-011-622)
• EMC Avamar 6.0 Product Security Guide (P/N 300-011-640)
• EMC Data Domain Product Overview
• EMC Data Domain Boost for Avamar
• EMC Avamar Data Store Site Prep Technical Specifications (P/N 300-007-104)
• EMC Technical Note Configuring VLAN Traffic Over Different Subnetworks (P/N 300-012-440)
• EMC Avamar: Business Deployment Considerations for Service Providers