Why use iSCSI over the WAN?

IT organizations have moved to appliance-based SAN arrays for their mass storage needs. Meanwhile, the creation of geographically distributed small offices and datacenters for redundancy/disaster recovery purposes has created the need for such storage arrays to remain synchronized across general purpose network links. Dell EqualLogic solutions use the iSCSI protocol for this purpose. Additional benefits of iSCSI include:

- Leverage existing storage applications like mirroring, backup, and disaster recovery without requiring modifications to those processes
- Utilize existing SCSI devices and existing IP networking infrastructure like WAN and MPLS
- Rely upon existing IT expertise and tools to manage the IP-based storage network
- Create a storage solution that is readily available to any application

The two primary uses for iSCSI over a WAN are remote storage calls from application servers and disk replication between SAN array devices. Application server to SAN array iSCSI generally occurs when the application only need occasionally access to the data on the SAN. This is particularly true with Internet-facing applications that may have a server per geography but only one set of shared data on a SAN. More often iSCSI crosses a WAN when two SAN arrays perform replications, both full (for newly deployed arrays) and partial for ongoing synchronization. Both uses of iSCSI are critical to provide ongoing access to data regardless of the network latency and constraints between datacenters. However, these actions over a WAN, with reduced bandwidth and high latency, often suffer from severely degraded performance, slowing business-critical operations. Typical application server to SAN array lookups are composed of many small SCSI commands. Even the largest file access may still be increasing the TCP data window minutes or hours into the transfer. This is less of an issue for full SAN replications where the transfers are generally larger, but any packet loss on the WAN will greatly decrease the maximum transfer rate until TCP scales its transmissions back up. Incremental replications, a standard feature of many SAN arrays, fall somewhere between the two in terms of performance across a WAN.

How can Blue Coat help?

While iSCSI provides SAN connectivity without dedicated cabling, it does not include any optimizations to address the latency and throughput constraints of a WAN link. Blue Coat Systems provides an end-to-end solution based on MACH5 (Multiprotocol Accelerated Caching Hierarchy) technology to regain performance, minimize bandwidth usage, and significantly reduce the time to complete iSCSI operations between locations. Blue Coat’s MACH5 Application Delivery Network (ADN) improves and accelerates iSCSI replication. Additional benefits include:

- Byte caching and compression technologies reduce bandwidth utilization by up to 95% allowing data transfers to complete in minutes or seconds instead of hours.
- When combined with protocol optimization provided by the Blue Coat ProxySG, which ensures full utilization of the link, the SAN array software’s TCP behavior is automatically managed in a way to optimize the TCP window size and send as much data in the shortest amount of time.
- Additionally, the Blue Coat solution also provides the ability to employ bandwidth management/QoS (quality of service) for any class of traffic to be appropriately prioritized.
- The Blue Coat solution is also the only solution capable of integrating into your existing IT infrastructure, allowing for flexible and quick deployment.
Why use Blue Coat with the Dell EqualLogic PS?

Dell EqualLogic storage arrays, known as the EqualLogic PS, utilize iSCSI and can be deployed in many environments. For example, an organization may have several remote locations that require additional SAN locally but require replication to a regional or core datacenter location. In addition, an organization may look to create replication of large data between datacenters. In each of these cases, iSCSI must make use of the WAN and therefore subject to the challenges mentioned above. By adding the Blue Coat ADN optimization device, known as the ProxySG, demand on the bandwidth and time to complete replications sets can be greatly reduced. The combined solution provides the following benefits:

-> Ease of deployment into existing network environments as there is virtually no network downtime for installation

-> Transparent to the end users while giving the optimum storage capacity and protection of data with replication

-> Reduction in time required to replicate data between locations

-> Best of breed products that can be relied upon for critical data storage and replication

Implementing the solution

The Dell EqualLogic PS and the Blue Coat ProxySG are deployed at the locations where the users or applications may access the arrays over a LAN. Typically, this would be at remote or branch offices that require additional storage capacity for end users and applications. Next, a PS and a ProxySG are deployed at the regional office or corporate datacenter. Using the built-in replication features of the Dell EqualLogic solution, iSCSI replication is configured between the locations. Finally, the Blue Coat ProxySG is easily configured to optimize and accelerate the iSCSI traffic as well as any additional applications that share the same bandwidth.

Consult the Dell EqualLogic documentation on specifics on the install and setup.

To configure the ProxySG, complete the following:

1. It is recommended that the unit at the remote or branch location be installed in a physically in-line configuration. It should be placed with one connection (LAN) to the switch that also has the Dell EqualLogic connection and the other connection (WAN) connected to the router that provides connectivity to the WAN. The regional or core datacenter can be either in-line or virtually in-line. Consult the ProxySG documentation on specifics for these options.

2. After the unit has been physically installed, attach a serial cable to the back of the unit and connected to a PC.

3. Using a terminal emulation application, start the setup wizard by hitting <enter> 3 times.

4. Depending on if you have Blue Coat Director or not, and how many devices you have to deploy, select either “Manual” or “Use Director” as the method to complete the configuration. The default is “Manual”.

5. After selecting “acceleration” as the “Solution to Implement” and “Physically in path” as the deployment type, complete the setup wizard to configure the networking parameters specific to the network that is to be used.

6. When prompted, do not enable acceleration at this point.
7. When finished, with a browser connect to the device at the address shown on the completion screen.

8. Log in using the user and password created during the setup wizard.

9. From the main dashboard, click Configuration and then Advanced Configuration as shown in the diagram:

This will launch a new browser window with the Advanced Configuration GUI.

10. Form the new GUI, select Services –> Proxy Services

11. In order to have the EqualLogic Replication traffic show up under a unique name for monitoring and reporting, add a new service called EQL-Replication. To add this new service, select the “New Service” button.

12. For the name, type EQL-Replication. For the Service Group, select Standard and then select TCP Tunnel as the Proxy. Leave the check boxes alone. In the Listeners section, select the “New” button and if you know the IP address of the regional branch office or datacenter array that the local array will contact, enter in that IP address. For the Port Range, enter 3260 and then select Intercept and OK. If there are more than one remote Array that could be contacted by the PS local to this proxy and the IPs are also known, repeat for all regional or datacenter arrays. If the IP addresses are not known, leave the Destination IP as “All” and complete the other steps as outlined.

13. Management of the Arrays happens on port 3003. Repeat the last 2 steps to add a new Service for EQL-Management.

14. Review the list of built-in Services and change the “Intercept” selection to “Bypass” or vice versa based on the application or services you would like optimized.

15. Be sure to click the “Apply” button when finished adding and editing the services.

16. No policy is required for this solution.

17. The default policy should be set to “Allow” if the setup wizard was used and ‘acceleration’ was indicated.

**Intercepting and Optimizing traffic**

When ready to begin with the optimization of the traffic, merely change the mode to Acceleration. This can be done via either of the following process:

1. From the Advanced Configuration GUI, click on Services -> Proxy Services.

2. At the top, deselect the check box for “Temporarily bypass all traffic.”

3. Click Apply

OR
4. From the original GUI, go to Configuration –> Acceleration –> Traffic Management

5. Change the radio button to have the “Acceleration Mode” selected.

Ensure that the ProxySG at the other side of the connection is also configured.

Verify Optimization

In order to verify that optimization is working, data will need to be sent. A quick way to do this is to perform a manual “Replication Set” from the PS Group Manager GUI. Assuming the PS is already configured with a volume, follow these steps:

1. Log into the PS Group Manager interface.
2. Go to the Group Monitoring section by clicking the “Group Monitoring” item from the menu set on the left.

3. Click the “Replication” tab if that is not the section that appears on the right side. A list of your configured Volumes will appear. If you do not have a list of Configured Volume Replication, consult the EqualLogic documentation on how to create this.

4. Select the Volume that you wish to perform the verification test with:

5. Right click on the selected entry and choose, “Create Replica Now”. Confirm that this is the action you want by clicking “Yes” when prompted.

6. The replication will begin between the selected replication partners.

Now it is time to log into the SG management GUI and verify that the optimization tunnel is in place.

7. Log into the SG management GUI using the credentials created above.

8. From the main screen, ensure that you are on the Monitor section by selecting the tab above.

9. The newly created EQL-Replication service will not be displayed until you select it as one to display. To get this service to display, click on the “Change services” button in the middle of the page.

10. Next select EQL-Replication as one of the items to display and click OK.

11. Now, you should see some activity for the EQL-Replication service if everything has been configured properly.
If you are not getting something in the chart for the EQL-Replication service, see the troubleshooting section below.

12. You may also go to the Advance Configuration section to see additional information on the optimization being performed. To get to the additional statistics, click the “Configuration” tab and then select the “Advanced Configuration” link at the bottom left side.

13. Once in the advanced configuration GUI, select the “Sessions” → “Active Sessions” menu option on the left on the “Statistics” tab. This view requires you to select the “Show” button in order to get data to be displayed.

14. If the replication set has completed by the time you look at the above view, you will have to go to the “ADN History” menu option to see the details of the test replica being created.

15. Once you have verified that the transaction is being captured by the SG appliances, you are ready to continue with the standard EqualLogic scheduling.
Troubleshooting

This section will attempt to cover any configuration settings that were not detailed above due to the complexity of the setting or these are not the default and could be used instead. In addition, this section will give some common configuration issues and recommended resolution.

SG Configuration – Advanced options

The configuration recommended is based on using the 5.4.x installation wizard and accepting the defaults. However, if an older version is utilized, the following will outline the required configuration option to accomplish the same result. Having a configuration other than the defaults or the options listed below may result in a non-functional optimization.

**Topic #1** – Open, Unmanaged ADN: Open, Unmanaged ADN is a concept that was introduced with SGOS 5.4.1 and does not require the use of an ADN Manager and only works with transparent tunnel. Furthermore Open ADN is when any ADN peer is allowed to create an ADN Tunnel with any other peer. For this solution, Open Unmanaged was the default if using the initial setup wizard. It is possible to have a successful tunnel created with an ADN Manager defined as well as unselecting “Allow transparent connection only within this managed network” on the ADN Manager itself. This would create what is referred to as Open, Managed ADN. Finally, with older versions of SGOS, the only option was Closed, Managed ADN. Closed ADN requires every peer to connect with the ADN Manager in order to become part of the ADN and thus establish tunnels.

None = Open, Unmanaged ADN

Self or IP Address = Open, Managed ADN

In older versions of SGOS, the only options were to have a specified IP Address or the unit becomes the ADN Manager (Self) = Closed ADN

Recommendation – any of the ADN manager options will work for this solution. Consult the Blue Coat documentation on when each should be used if concerned about this selection as certain other uses of this same ADN peer within your environment might require the use of a Closed, Managed ADN (not the default).

**Topic #2** – Use with WCCP: Although the default configuration is to deploy the ProxySG physically in-line, a virtually in-line deployment with WCCP is also supported. Nothing is special in order to support the EqualLogic solution.

Recommendation – WCCP may be used. Consult the Blue Coat WCCP deployment guides for specific information if you have further questions concerns.
**Topic #3** – Reflect Client IP: Reflect client IP should only be used if the network topology can support that architecture. Please also be aware of the differences in the configuration options between SGOS versions prior to 5.3.x and those after 5.3.x.

Recommendation – only utilize “Reflect Client IP” for environments that can support it. Consult the upgrade guide for any version 5.3 and beyond for more details.

**Topic #4** – Tunnel isn’t getting created: If you go thru the setup and verification test as outlined above and the ADN tunnel is not created, follow some of the basic troubleshooting steps to help resolve the issue.

Recommendation – First, ensure that ADN is enabled. Next, make sure the Eql-Replication service is set to “Intercept”. Ensure that the service listener was created properly and there isn’t an error in the hosts that are designated for the service.

**Topic #5** – Conflict of default gateway MAC address: If the SG (running SGOS prior to 5.4.x) is inline and deployed behind a L3 device that is also designated as the default gateway of the EqualLogic PS, the EqualLogic may erroneously decide that the SG is its default gateway and ignore the configured setting. It makes this determination based on source MAC address of the packets it receives from the SG. This issue will not show up if you view the Group Manager GUI list of gateways, but will be visible by viewing the default gateway list via the CLI. Replication may run successfully for days or longer without experiencing any problems. However, if the replication is paused or restarted, no errors are given by the replication will fail. To clear the issue and allow for a successful replication is to disable and then re-enable all active ports on the PS. This issue is resolved in SGOS version 5.4.x and beyond.

Recommendation – The best way to avoid or resolve this issue is to upgrade the SGOS version to a version that has this resolved. If an upgrade is not possible, then the only work around to avoid having to reset the active ports is to change the configuration of the PS to have the SG be its default gateway. In SGOS version 5.4.x and beyond, there is an added feature called “Trust Destination MAC”. This feature is only applicable to in-line, bridged deployments. It is enabled by default and can not be disabled. Consult the SGOS version 5.4.x release notes for more details.