NetBackup 7.6 Feature Briefing

Targeted Auto Image Replication

Version number: 1.1

Issue date: 29th October 2013

This document describes a feature introduced in NetBackup 7.6 and available in this and higher releases.

If you have any feedback or questions about this document please email them to **IMG-TPM-Requests@symantec.com** stating the document title and version number.

Confidence in a connected world. ✓Symantec.

Feature Description

Auto Image Replication is a NetBackup feature that protects against site outages by replicating backups between NetBackup domains and cataloging the replicated images in the target domains. It was introduced in NetBackup 7.1 and can be used with many types of disk storage including media server deduplication (MSDP), PureDisk deduplication (PDDO) and some 3rd party OpenStorage devices.

Auto Image Replication also supports simple one-to-one, many-to-one and one-to-many replication configurations. Replication is based on disk storage servers with each source disk storage server being configured with access credentials for one or more target disk storage servers

Where one-to-many replication is used the default behavior is to replicate images to all of the target storage servers associated with a source storage server. Whether an image is imported into a particular target domain will depend on whether an import Storage Lifecycle Policy exists in that domain.

In NetBackup 7.6, the Targeted Auto Image Replication feature allows selective replication of images from a source disk storage server to specific disk storage servers in individual target domains, allowing the same disk pool to be used for images being sent to different target domains without generating unnecessary network traffic.

Targeted Auto Image Replication works by leveraging the new "master server to master server communication layer" introduced in NetBackup 7.6 to establish a trust relationship between source and target domain master servers that allows the backup administrator in the source domain configuring a replication operation in a Storage Lifecycle Policy to select a particular target domain and import Storage Lifecycle Policy for a given replication operation.

Business Value

Targeted Auto Image Replication provides clear visibility into the target domain, when configuring the source domain. When configuring a Storage Lifecycle Policy to use Targeted AIR the user now may:

- Target a specific Master Server by name
- Target a specific SLP in that master server for import
- Be assured that NetBackup has confirmed the replication topology chosen will work and provide the expected behavior

In addition to the above, the new Data Classification "Any" may be used by the Import SLP in the target domain. This Data Classification is capable of importing any data classification and preserving the source domain's data classification in the target domain.

By using Targeted Auto Image Replication functionality, the user no longer needs a matching Storage Lifecycle Policy name or a matching data classification across all participating domains. In addition, when the source Storage Lifecycle Policy is configured, its storage configuration is validated against the target domains for compatibility, simplifying the configuration process.

Targeted Auto Image Replication allows users with one-to-many and many-to-many replication topologies the following benefits:

- Select a subset of available targets for replication within any given SLP
- Each target chosen is allowed to use a different retention to satisfy different SLAs for different business needs (i.e. short to medium retention offsite "hot standby" and long-term DR, plus test/dev domain, etc.)
- Allows unnecessary network traffic to be eliminated without requiring additional disk storage in the source domain

By using Targeted Auto Image Replication, the user is given a way to add new target devices as old devices are "aged" out of service. For example, when replacing a full target device with a newer generation of hardware with much higher capacity, the Targeted SLP allows a user to have both targets configured at the same time at the storage layer to complete "in-flight" replications and start using the new device in parallel. This eliminates any interruption in service for routine maintenance scenarios.

Finally, Targeted Auto Image Replication provides a notification capability from the target master server to its source master server, in the event that the target master is unable to import an image. The existing import errors posted to the master server's "Problems Report" are now duplicated to the source master server's "Problems Report". This additional notification provides a continuous feedback to the source domain of any risk of failure to import, as well as any device configuration changes which may have broken the replication configuration.

Underlying Principles

Targeted Auto Image Replication is based on a trusted relationship between the master servers of two separate domains. Information about the remote master server is stored on the local master server and information is exchanged between the two using the NetBackup `nbsl` service.

When a new replication operation is added to a Storage Lifecycle Policy in the source domain the backup administrator can select the target domain's master server from a list of trusted master servers. Once the target master server is selected a list of relevant import Storage Lifecycle Policies in the target domain is generated and the administrator can then select the required import Storage Lifecycle Policy.

When the Storage Lifecycle Policy in the source domain executes a replication operation it passes the name of the target import SLP to the target domain. If the target import Storage Lifecycle Policy does not exist (for example it has been deleted) it will be automatically created unless "Auto create A.I.R. Import SLP" is set to "No" in the target domain master server's SLP Parameters, in which case the replication operation will fail.

Note: In NetBackup 7.6 the LIFECYCLE_PARAMTERS file no longer exists. Instead SLP parameters are stored under the master server host properties in the relational database and are modified from the Administration GUI by going to Host Properties -> Master Server -> SLP Parameters.

Guided Tour

The trust relationship between two master servers can be established from a single master server provided the login credentials for the target master server are known to the source domain administrator. In this case the whole configuration from both source and target masters can be done through the host properties on the source master server by going to host properties -> master server -> servers and selecting "Add" on the "Trusted Master Servers" tab (see Figure 1).
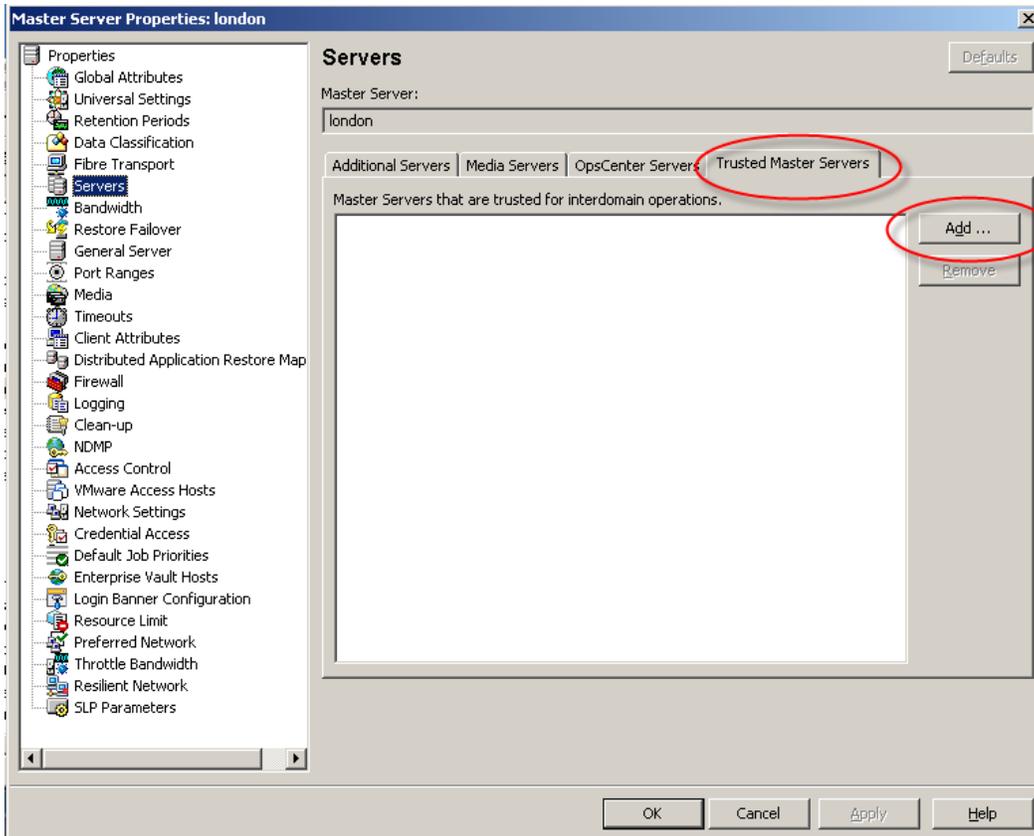
Figure 1 - Adding a trusted master server

You will be prompted for the master server name, user name, and password (see Figure 2).
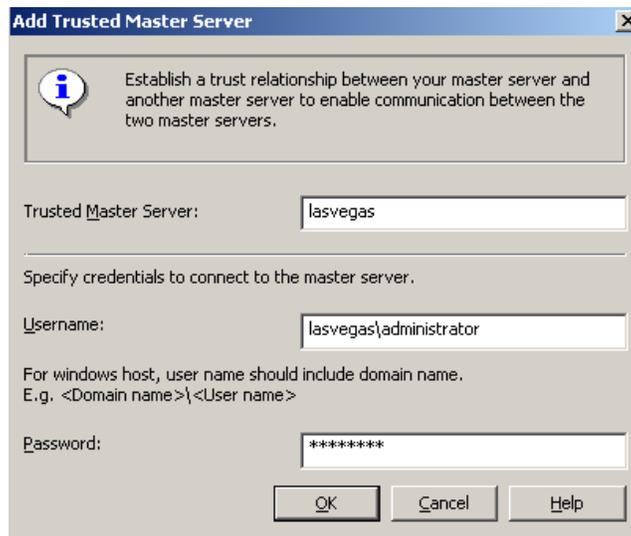

Figure 2 – Entering the trusted master server credentials

Note that the credential information is only used only to validate the remote connection and add details of the source master server to the target master server. It is not stored anywhere.

The process to remove a trusted master server is identical to the process used to add it and the current access credentials must be added to complete the removal.

If the credentials for the source and target domains cannot be shared for operational security reasons the trusted master server relationship can be established independently on each master server by running the command:

```
nbseccmd –setuptrustedmaster –add  -masterserver  <local master>
–remotemasterserver <remote master> -localonly
```

Where <local master> and <remote master> are the names of the local are remote master servers. No login credentials need to be entered when this command is run.

Note: A warning message will be generated on the first host the command is run on. This is normal and simply reminds the user that the corresponding command still needs to be run on the other master server.

Once the remote master server is added the trust master server can be interrogated to determine the storage servers available in a target domain when adding the replication credentials to the source storage server. First go to Media and Device Management -> Credentials -> Storage Servers and select the source storage server. Then go to the replication tab (see Figure 3).
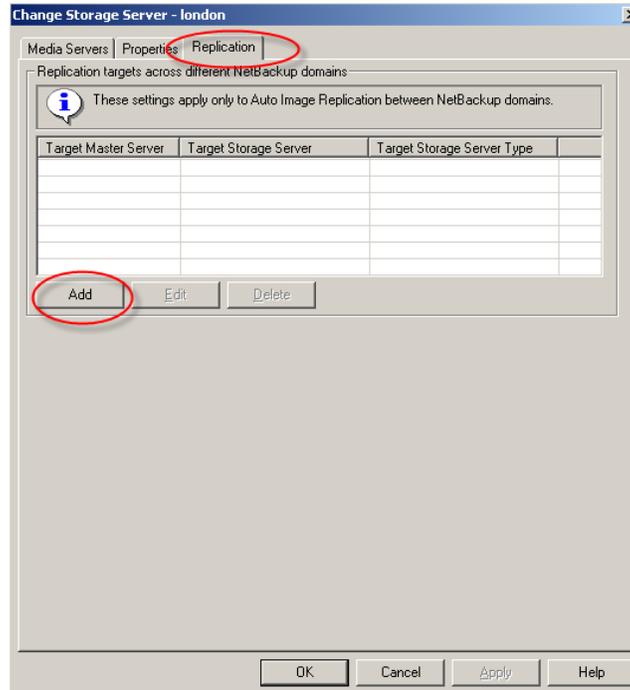
Figure 3 - Adding a replication target

Selecting "add" will open the add dialogue box (see Figure 4). Select the target master server from the available list. Then select the target storage server type and target storage server name (this will be automatically populated if there is only one supported storage server in the target domain).
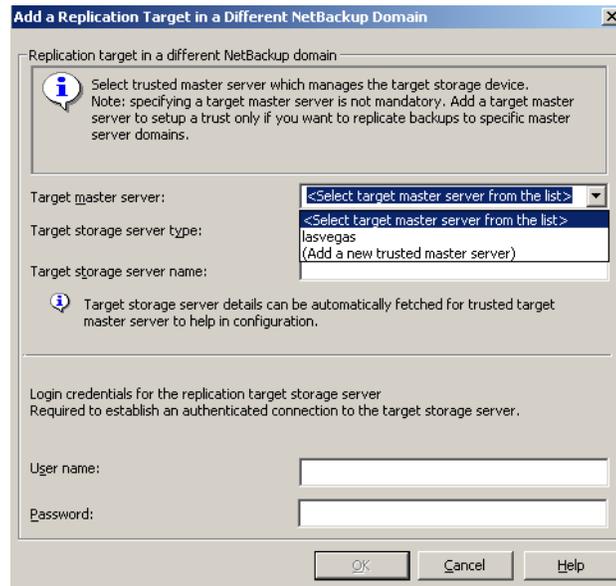

Figure 4 - Adding replication credentials using information from a trusted master server.

Note that it is possible to add a new trusted master server at this point without needing to go to the master server host properties.

Add the storage server credentials and select OK to save the changes.

When defining the replication storage operation the trusted master server can be selected and used to provide the names of import Storage Lifecycle Policies available in the target domain (see Figure 5).
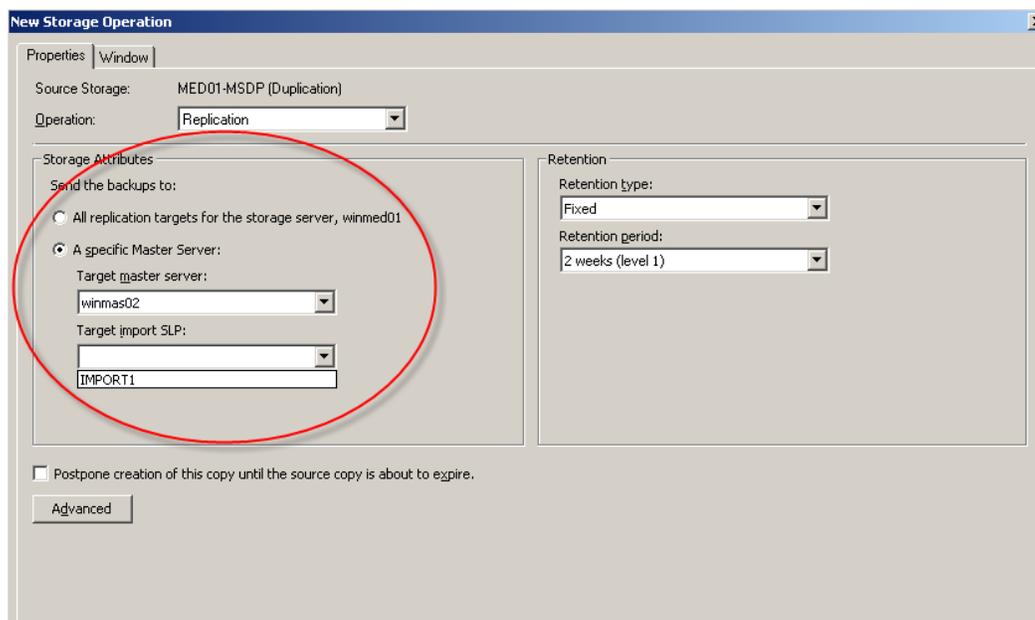

Figure 5 - Creating a replication operation using a trusted master server

Licensing and support considerations

Storage Lifecycle Policies and Auto Image Replication are licensed as part of the Data Protection Optimization Option.

This feature requires both the source and target domain master servers to be running NetBackup 7.6 or above. In NetBackup 7.6 this feature is only supported with Symantec storage solutions (MSDP and PDDO) and is not available for 3rd party OpenStorage devices.

Related documents

NetBackup Administrator's Guide, volume I

Best practices for SLPs and AIR in NetBackup 7.6

About Symantec:

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at **www.symantec.com**.