Customer Logo

In partnership with

Business Partner Logo

StorageGRID Acceptance Test Plan Draft

StorageGRID 11.x

July 2019

TABLE OF CONTENTS

[1 Official Signoff of Acceptance Test Plan Definition 5](#_Toc13511114)

[2 Introduction 6](#_Toc13511115)

[2.1 Assumptions and Dependencies 6](#_Toc13511116)

[3 Test Plan 7](#_Toc13511117)

[3.1 Grid Topology and Configuration 7](#_Toc13511118)

[3.2 Admin Account, and Tenant Setup 9](#_Toc13511119)

[3.3 S3 Ingest, Retrieve, and Delete 9](#_Toc13511120)

[3.4 Policy Management 11](#_Toc13511121)

[3.5 Anonymous/Bucket Anonymous Request via Web Browser 12](#_Toc13511122)

[3.6 Resiliency and Failure Handling 13](#_Toc13511123)

[4 Test Results Summary 14](#_Toc13511124)

[Version History 15](#_Toc13511125)

LIST OF TABLES

[Table 1) Grid Configuration verification. 9](#_Toc13511104)

[Table 2) Root storage tenant setup verification. 9](#_Toc13511105)

[Table 3) S3 ingest setup verification. 10](#_Toc13511106)

[Table 4) S3 retrieve setup verification. 10](#_Toc13511107)

[Table 5) S3 delete setup verification. 11](#_Toc13511108)

[Table 6) Multisite topology and active policy setup verification. 11](#_Toc13511109)

[Table 7) Ingest rule setup verification. 12](#_Toc13511110)

[Table 8) Bucket Anonymous Requst via web browser. 13](#_Toc13511111)

[Table 9) Node failure handling verification. 13](#_Toc13511112)

[Table 10) Acceptance test summary results. 14](#_Toc13511113)

# Official Signoff of Acceptance Test Plan Definition

We agree with regards to the definition as outlined in this Acceptance Test Plan (“ATP”). We agree that this document defines the complete scope for the ATP of StorageGRID system as specified by Lintasarta and NetApp. All future requests for more testing are considered to be outside the scope of this ATP.

|  |  |
| --- | --- |
| Representative for <customer-name> |  |
| Signature |  |
| Name (printed) |  |
| Title or Position |  |
| Date |  |

# Introduction

NetApp conducts acceptance testing to verify that implementation activities for StorageGRID software components in Lintasarta environments were completed successfully. The acceptance testing consists of basic checklists that align with the deployment methodology for the NetApp StorageGRID product. Execution of these acceptance checks is witnessed by NetApp and Lintasarta and, optionally, by a MasterSystem representative. The witnessed test results are delivered to Lintasarta and constitute the basis for formal acceptance by Lintasartaof the respective implementation deliverables.

The StorageGRID is deployed across two sites, data center at Taman Tekno and disaster recovery at TBS

This test plan documents the test cases used to demonstrate that the StorageGRID system has been successfully deployed and is fully operational.

The objectives of this document are as follows:

* To clearly define the complete scope of the Installation and Operational Acceptance Tests for the NetApp StorageGRID.
* To acknowledge and document the successful deployment of the NetApp StorageGRID within the Lintasartaenvironment.

## Assumptions and Dependencies

Successful completion of acceptance testing relies on the following assumptions:

* The NetApp StorageGRID is fully deployed and is in an operational state.
* Amazon Simple Storage Service (Amazon S3) Browser is installed on a Windows workstation with network connectivity to NetApp StorageGRID system.
* Amazon Web Services (AWS) CLI is installed on a Linux workstation with network connectivity to NetApp StorageGRID system.
* TCP/IP connectivity has been verified within customer environment.
* Access to the NetApp StorageGRID network is made available to support browsing of the GRID Management Interface (GMI).
* Customer network administrator is available to disable network port for network redundancy test.

# Test Plan

The test cases in this Test Plan are intended to verify proper installation, configuration, and integration of the NetApp StorageGRID software.

## Grid Topology and Configuration

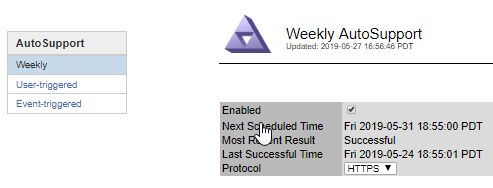
This section discusses the procedure for reviewing grid topology.

### Prerequisite

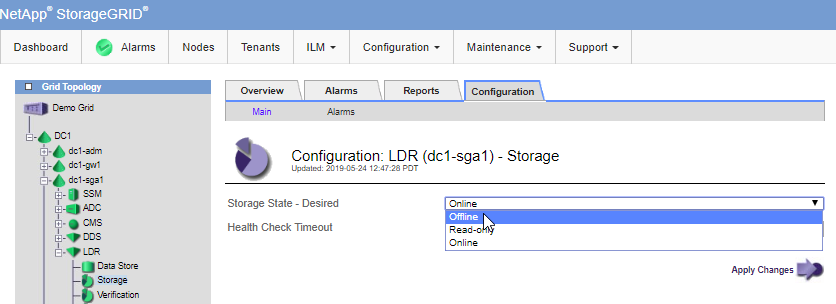
The StorageGRID system is configured and operational as described in section 2.1.

### Procedure

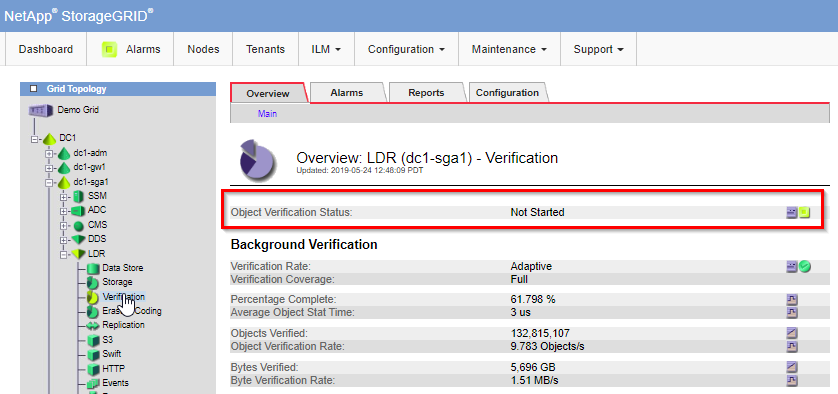
1. Log in to the Grid Management Interface (GMI) using root account or other account with root privileges.
2. On the Dashboard page, confirm Heath status with no unexpected alarm.
3. Navigate to Maintenance > License and confirm that the ‘Storage Capacity (terabyte)’ license matches with the Sales Order.
4. Navigate to Support > Grid Topology and confirm that the following display as expected:
5. Number of sites
6. Number and type of nodes per site
7. The total installed storage capacity at grid level and each individual site. The total installed storage capacity should be approximately 70% to 75% of licensed capacity.
8. All nodes and services are online
9. Navigate to Configuration > Grid Options and verify that the options settings meet customer requirements.
10. Navigate to Support > AutoSupport and verify that ‘Weekly AutoSupport’ and ‘Event-triggered’ is enabled and successfully sent.



1. For StorageGRID appliance, use NetApp SANtricity® Storage Manager to verify that autosupport is enabled and an email alert is set up on each Appliance storage controller.
2. Navigate to Configuration > Email Server, select Server, confirm that email server is set up. Configure ‘Test Email’ to trigger ‘Send Test Email’. Confirm that test email is received.
3. Navigate to Configuration > Email Server, select Lists and confirm email Group and Recipients are set up.
4. Navigate to Configuration > Notifications, confirm that the email list is set up to receive email alerts from the grid.
5. Include Notice Severity Levels for the test in step 9.
6. Trigger an alarm verifying that the email notification was sent out as expected.
7. Navigate to Support > Grid Topology.
8. Navigate to a Storage Node, select LDR > Storage.
9. On Storage Page, Select Configuration tab.
10. Set “Storage State – Desired” to ‘Offline’ and Apply Changes.



1. Confirm that an alarm is triggered under LDR > Verification.



1. Confirm that Grid notification email is received by recipients and configured in step 9 and 10.
2. Set the ‘Storage State – Desired’ to Online to clear this alarm
3. For a grid with three or more sites, Navigate to Configuration > Link Cost, verify that the link cost value between sites are set up based on customer site preference.
4. Record the result (Table 2).

Table ) Grid Configuration verification.

|  |  |
| --- | --- |
| Expected Results | PASS/FAIL |
| Grid is healthy with no alarm |  |
| Grid license matches with StorageGRID software sales order |  |
| Deployed Grid topology matches proposed design. |  |
| All Grid nodes and service are online. |  |
| Grid options are configured and meet customer requirements. |  |
| StorageGRID Autosupport is enabled and sent successfully. |  |
| StorageGRID Appliance’s storage controller autosupport is enabled and email alert is set up. |  |
| StorageGRID Email Server, list, and notification are configured. |  |
| The email notification is successfully received. |  |
| Alarm is clear after Storage State is set to Online. |  |

## Admin Account, and Tenant Setup

This section outlines the procedures for reviewing admin accounts, and root storage tenants.

### Root Storage Tenants

Use the following steps to review root storage tenants.

Procedure

1. Navigate to Tenants > Tenant Accounts.
2. Create an S3 account. Record the root tenant password and numeric ID.

Table ) Root storage tenant setup verification.

|  |  |
| --- | --- |
| Expected Results | PASS/FAIL |
| S3 root storage tenant accounts are created and configured. |  |

## 

## S3 Ingest, Retrieve, and Delete

This section discusses how to review S3 ingest, retrieve, and delete.

### S3 Ingest

Use the following steps to review S3 ingest.

#### Procedure

1. In the GMI, navigate to Nodes.
2. Select Grid and then Objects.
3. Zoom in to the recent seconds and observe the rate of “S3 Ingest and Retrieve.”
4. Using the AWS CLI or S3 Browser, ingest a few test objects into the test bucket.
5. In the GMI, navigate to Nodes.
6. Select Grid and then Objects.
7. Zoom in to the recent seconds and observe the increase in the rate of “S3 Ingest and Retrieve.”
8. In the GMI, navigate to ILM > Object Metadata Lookup.
9. Perform an object lookup by using the following syntax: bucket name/S3 key name. Record the content block identifier returned (Table 8).

Table ) S3 ingest setup verification.

|  |  |
| --- | --- |
| Expected Results | PASS/FAIL |
| The “S3 Ingest and Retrieve” rate increased when objects were ingested |  |
| Confirm that the object retrieved is identical to the object ingested earlier |  |

### S3 Retrieve

Use the following steps to review S3 retrieve.

#### Procedure

1. In the GMI, navigate to Nodes.
2. Select Grid and then Objects.
3. Zoom in to the recent seconds and observe the rate of “S3 Ingest and Retrieve.”
4. Using the AWS CLI or S3 Browser, retrieve the test objects previously ingested into the test bucket.
5. In the GMI, navigate to Nodes.
6. Select Grid and then Objects.
7. Zoom in to the recent seconds and observe the increase in the rate of “S3 Ingest and Retrieve”. Record the result in Table 9.

Table ) S3 retrieve setup verification.

|  |  |
| --- | --- |
| Expected Results | PASS/FAIL |
| The “S3 Ingest and Retrieve” rate increased when objects were ingested |  |
| Confirm that the object retrieved is identical to the object ingested earlier (use md5sum). |  |

### S3 Delete

Use the following steps to set up S3 delete.

#### Procedure

1. In the GMI, navigate to Nodes.
2. Select Grid and then Objects.
3. Zoom in to the recent seconds and observe the rate of “S3 Ingest and Retrieve”.
4. Using the AWS CLI or S3 Browser, delete the test object previously ingested into the test bucket.
5. In the GMI, navigate to Nodes.
6. Select Grid and then Objects.
7. Zoom in to the recent seconds and observe the increase in the rate of “S3 Ingest and Retrieve”.
8. In the GMI, navigate to ILM > Object Metadata Lookup.
9. Perform an object lookup by using the following syntax: bucket name/S3 key name. The search should return Object Not Found.
10. Record the result in Table 10.

Table ) S3 delete setup verification.

|  |  |
| --- | --- |
| Expected Results | PASS/FAIL |
| The “S3 Ingest and Retrieve” rate increased when objects were deleted |  |
| The object is not found in the object lookup |  |

## Policy Management

This section discusses how to review policy management.

### Review Multisite Topology and Active Policy

Use the following steps to review multisite topology and active policy configuration.

#### Prerequisite

The StorageGRID system has been configured with storage pool, erasure coding profiles (if applicable), rules, and ILM policy based on customer requirements.

#### Procedure

1. In the GMI, navigate to Support > Grid Topology, confirm all nodes and services are up.
2. In the GMI, navigate to Grid Configuration > Link Cost, review the link cost groups.
3. If applicable, Navigate to ILM > Storage Grades, review the storage grades.
4. Navigate to ILM > Policies.
5. Review the preconfigured storage pools.
6. Review the preconfigured rules.
7. Review the preconfigured active ILM policy (Table 11).

Table ) Multisite topology and active policy setup verification.

|  |  |
| --- | --- |
| Expected Results | PASS/FAIL |
| Storage Pools and Erasure Coding profile (if applicable) are configured to per customer requirements |  |
| Rules and ILM policy are configured per customer requirements. |  |

### Ingest Rule

Use the following steps to review the ingest rule.

#### Precondition

The ingest rule is in the active ILM policy.

#### Procedure

1. Using the AWS CLI or S3 Browser, ingest a test object into the test bucket.
2. In the GMI, navigate to Nodes.
3. Select Grid and then Objects.
4. Zoom in to the recent seconds and observe the increase in the rate of “S3 Ingest and Retrieve.”
5. In the GMI, select ILM > Object Metadata Lookup.
6. Search for the object by using the following syntax: bucket name/object name.
7. Record the copy locations returned from the query.
8. Log in to Admin Node using SSH:
9. Login user=admin, password can be found in the recovery package.
10. Enter ‘su’ and use the same Admin password
11. Find the rule applied to this object, replace the <object-name> with actual object name:

grep ‘<object-name>’ /var/local/audit/export/audit.log | grep ORLM

1. Record the result in Table 12.

Table ) Ingest rule setup verification.

|  |  |
| --- | --- |
| Expected Results | PASS/FAIL |
| Confirm that the object copy locations meet the ingest rule locations specified in the active policy |  |
| Confirm that the correct rule is applied to the object. |  |

If there are multiple rules in active ILM policy, you can repeat this test for each rule.

## Anonymous/Bucket Anonymous Request via Web Browser

#### Procedure

1. Login to S3CMD 🡪 /opt/s3cmd
2. Create JSON to enable access to Bucket

Vi anonymous\_access\_uat.json

{

"Statement": [

{

"Effect": "Allow",

"Principal": "\*",

"Action": [

"s3:GetObject",

"s3:ListBucket"

],

"Resource": [

"urn:sgws:s3:::uat",

"urn:sgws:s3:::uat/\*"

]

}

]

}

1. Save anonymous\_access\_uat.json
2. Run 🡪 s3cmd setpolicy anonymous\_access.json s3://uat
3. Inget file via S3 Browser to “uat” bucket
4. Access via browser https://182.23.67.97:8082/uat/???

Table 8) Bucket Anonymous Requst via web browser.

|  |  |
| --- | --- |
| Expected Results | PASS/FAIL |
| Confirm that the object can be access from Web Browser without authentication |  |

## Resiliency and Failure Handling

This section discusses how to review resiliency and failure handling.

### Node Failure

Verify that the failure of a storage node does not affect object access.

#### Procedure

1. Navigate to ILM > Object Metadata Lookup.
2. Search for the object identifier.
3. Locate the storage nodes where the object is stored.
4. Choose one of the storage nodes and shut it down.
5. Using the AWS CLI, retrieve the object ingested during the last test case.
6. Compare the object retrieved with the original ingested object (Table 15).

Table ) Node failure handling verification.

|  |  |
| --- | --- |
| Expected Results | PASS/FAIL |
| The operation of the StorageGRID system is unaffected. |  |

# Test Results Summary

This section summarizes the acceptance test results. It also provides for the sign‑off of the test results by all key stakeholders.

Table 10 provides a summary of the results.

Table ) Acceptance test summary results.

|  |  |
| --- | --- |
| Expected Results | PASS/FAIL |
| Grid Topology and Configuration |  |
| Identity Federation Integration, Admin Account, and Tenant Setup |  |
| S3 Ingest, Retrieve |  |
| Policy Management |  |
| Resiliency and Failure Handling |  |
| Overall test plan result |  |

Version History

|  |  |  |
| --- | --- | --- |
| Version | Date | Document Version History |
| 1.0 | July 2019 | Initial Release |

Refer to the [Interoperability Matrix Tool (IMT)](http://mysupport.netapp.com/matrix) on the NetApp Support site to validate that the exact product and feature versions described in this document are supported for your specific environment. The NetApp IMT defines the product components and versions that can be used to construct configurations that are supported by NetApp. Specific results depend on each customer’s installation in accordance with published specifications.

Copyright Information

Copyright © 2019 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.