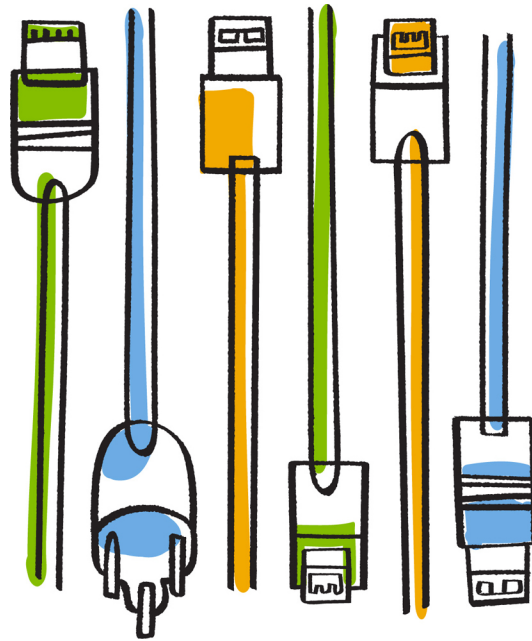




## StorageGRID® Webscale 10.2

### Swift Implementation Guide



NetApp, Inc.  
495 East Java Drive  
Sunnyvale, CA 94089  
U.S.

Telephone: +1 (408) 822-6000  
Fax: +1 (408) 822-4501  
Support telephone: +1 (888) 463-8277  
Web: [www.netapp.com](http://www.netapp.com)  
Feedback: [doccomments@netapp.com](mailto:doccomments@netapp.com)

Part number: 215-10140\_A0  
December 2015



# Contents

<b>OpenStack Swift API support in StorageGRID Webscale .....</b>	<b>4</b>
History of Swift API support in StorageGRID Webscale .....	4
How StorageGRID Webscale implements the Swift REST API .....	4
<b>Swift REST API supported operations .....</b>	<b>5</b>
General information about Swift info, auth, and storage URLs .....	5
Error responses to Swift API operations .....	7
Account operations .....	8
Container operations .....	9
Object operations .....	12
OPTIONS method .....	15
Operations tracked in the audit logs .....	15
<b>Configuring tenant accounts and connections .....</b>	<b>16</b>
Creating tenant accounts for Swift .....	16
How client applications use HTTPS connections .....	17
Identifying IP addresses for API Gateway Nodes and Storage Nodes .....	17
Port numbers on API Gateway Nodes and Storage Nodes for Swift .....	18
<b>Configuring security for the REST API .....</b>	<b>19</b>
How the StorageGRID Webscale system implements security for the REST API ...	19
Configuring a custom server certificate .....	20
Reverting a custom server certificate to the default certificate .....	22
Copying the StorageGRID Webscale system's CA certificate .....	22
How client applications use certificates for security with REST APIs .....	23
Supported hashing and encryption algorithms for TLS libraries .....	23
<b>Testing your connection in the Swift API configuration .....</b>	<b>25</b>
<b>Monitoring and auditing operations .....</b>	<b>27</b>
Viewing HTTPS transactions for Swift objects .....	27
Viewing information about data objects .....	28
Accessing and reviewing audit logs .....	28
<b>Copyright information .....</b>	<b>30</b>
<b>Trademark information .....</b>	<b>31</b>
<b>How to send comments about documentation and receive update notifications .....</b>	<b>32</b>
<b>Index .....</b>	<b>33</b>

## OpenStack Swift API support in StorageGRID Webscale

---

Support for the OpenStack Swift Representational State Transfer Application Programming Interface (REST API) enables client applications developed for OpenStack Swift to store and retrieve objects on a StorageGRID Webscale system. Before using the API, you might benefit by understanding its implementation in StorageGRID Webscale.

StorageGRID Webscale supports the following versions:

Item	Version
Swift specification	OpenStack Swift Object Storage API v1 as of November 2015
HTTP	1.1 For details about HTTP, see HTTP/1.1 (RFC 2616).

### Related information

[OpenStack: Object Storage API](#)

## History of Swift API support in StorageGRID Webscale

Understanding the initiation of and any changes to the support for the Swift API in the StorageGRID Webscale system might help you design your implementation.

The following table documents the StorageGRID Webscale system support for the Swift API:

Date	Release	Comments
December 2015	10.2	Initial support of the Swift API by the StorageGRID Webscale system. The currently supported version is OpenStack Swift Object Storage API v1.

## How StorageGRID Webscale implements the Swift REST API

A client application can use Swift REST API calls to connect to storage nodes and API Gateway nodes to create containers and to store and retrieve objects. This enables service-oriented applications developed for OpenStack Swift to connect with on-premises object storage provided by the StorageGRID Webscale system.

To manage objects, the StorageGRID Webscale system uses information lifecycle management (ILM) rules.

For information about ILM rules, see the *Administrator Guide*.

### Related information

[StorageGRID Webscale 10.2 Administrator Guide](#)

## Swift REST API supported operations

---

The StorageGRID Webscale system supports most operations in the OpenStack Swift API. If you are integrating Swift REST API clients with StorageGRID Webscale, understanding the implementation details for account, container, and object operations is helpful.

### Operations supported in StorageGRID Webscale

The following Swift API operations are supported:

- [Account operations](#) on page 8
- [Container operations](#) on page 9
- [Object operations](#) on page 12

### Common response headers for all operations

The StorageGRID Webscale system implements all common headers for supported operations as defined by the OpenStack Swift Object Storage API v1.

### Related concepts

[OpenStack Swift API support in StorageGRID Webscale](#) on page 4

### Related information

[OpenStack: Object Storage API](#)

## General information about Swift info, auth, and storage URLs

StorageGRID Webscale supports several Swift API endpoint types.

These Swift API endpoints are:

- info URL
- auth URL
- storage URL

### Swift capabilities and limitations with info URL

The capabilities and limitations of the StorageGRID Webscale Swift implementation can be queried through the Swift info URL. You obtain this information by issuing a GET request to the StorageGRID Webscale Swift base URL with the `/info` path.

```
https://<FQDN | IP>:<Swift_Port>/info/
```

The StorageGRID Webscale implementation of Swift allows unauthenticated access to the info URL.

A GET request to the info URL yields the capabilities of the Swift implementation as a JSON dictionary. A client tool can parse the returned JSON response to determine the capabilities of the implementation and employ them as constraints for subsequent storage operations.

## User authentication with auth URL

A client can authenticate a tenant user and procure a Swift token from the Swift auth URL. A successful authentication request yields a token and a storage URL, which are required for access on a StorageGRID Webscale a CLB service on the Gateway Node or LDR service on a Storage Node.

```
https://<FQDN | IP>:<Swift_Port>/auth/v1.0/
```

The credentials include the user name and password as parameters and must be provided using request headers as follows:

- X-Auth-User : <Tenant\_Account\_ID>:<Username>
- X-Auth-Key : <Password>

The Swift tenant account information is used in the authentication process and consists of one of the following:

- If Identity Federation is enabled for the tenant account (for Active Directory or LDAP configurations), you should provide the username and password of the federated user from the AD or LDAP server. Alternatively, LDAP users can be referred to with their domain name, for example, X-Auth-User: <Tenant\_Account\_ID>:<Username@Domain\_Name>
- For local accounts when LDAP is not configured, you should use "swiftadmin" as the user name and the password provided during tenant account creation.

A valid user name and password combination yields a valid token and storage URL through response headers as shown in the following:

```
X-Storage-Url    : https://<FQDN | IP>:<Swift_Port>/v1/<Tenant_Account_ID>
X-Auth-Token     : token
X-Storage-Token  : token
```

By default, the token is valid for 24 hours from generation time.

Tokens are generated for a specific tenant account. A valid token for one account does not authorize a user to access another account.

## Swift API operations with storage URL

A client application can issue Swift REST API calls to perform supported account, container, and object operations against a CLB service on the Gateway Node or LDR service on a Storage Node. Storage requests can be addressed to the URL that is returned by the auth request in the X-Storage-Url response header. The request must include the X-Auth-Token header and value returned from the auth request.

```
https://<FQDN | IP>:<Swift_Port>/v1/
<Tenant_Account_ID>[/container][ /object]
```

Because StorageGRID Webscale uses an eventually-consistent data model, some storage response headers that contain usage statistics might not reflect accurate numbers for recently modified objects. It might take a few minutes for accurate numbers to appear in these headers.

The following response headers are examples of those that contain usage statistics:

- X-Account-Bytes-Used
- X-Account-Object-Count

- X-Container-Bytes-Used
- X-Container-Object-Count

For details about responses, see information about account, container, and object operations.

#### Related references

[Account operations](#) on page 8

[Container operations](#) on page 9

[Object operations](#) on page 12

[Port numbers on API Gateway Nodes and Storage Nodes for Swift](#) on page 18

## Error responses to Swift API operations

Understanding the possible error responses can help you troubleshoot operations.

The following HTTP status codes might be returned when errors occur during an operation:

Swift error name	HTTP status
AccountNameTooLong, ContainerNameTooLong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadataNameTooLong, MetadataValueTooBig, MissingSecurityHeader, ObjectNameTooLong, TooManyContainers, TooManyMetadataItems, TotalMetadataTooLarge	400 Bad Request
AccessDenied	403 Forbidden
ContainerNotEmpty, ContainerAlreadyExists	409 Conflict
InternalError	500 Internal Server Error
InvalidRange	416 Requested Range Not Satisfiable
MethodNotAllowed	405 Method Not Allowed
MissingContentLength	411 Length Required
NotFound	404 Not Found
NotImplemented	501 Not Implemented
PreconditionFailed	412 Precondition Failed
ResourceNotFound	404 Not Found
Unauthorized	401 Unauthorized
UnprocessableEntity	422 Unprocessable Entity

## Account operations

The following Swift API operations are performed on accounts.

Operation	Implementation
GET account	<p>Retrieves the container list associated with the account and account usage statistics.</p> <p>The following request parameter is required:</p> <ul style="list-style-type: none"><li>Account</li></ul> <p>The following request header is required:</p> <ul style="list-style-type: none"><li>X-Auth-Token</li></ul> <p>The following supported request query parameters are optional:</p> <ul style="list-style-type: none"><li>Delimiter</li><li>End_marker</li><li>Format</li><li>Limit</li><li>Marker</li><li>Prefix</li></ul> <p>A successful execution returns the following headers with an “HTTP/1.1 204 No Content” response if the account is found and has no containers or the container list is empty; or an “HTTP/1.1 200 OK” response if the account is found and the container list is not empty:</p> <ul style="list-style-type: none"><li>Accept-Ranges</li><li>Content-Length</li><li>Content-Type</li><li>Date</li><li>X-Account-Bytes-Used</li><li>X-Account-Container-Count</li><li>X-Account-Object-Count</li><li>X-Timestamp</li><li>X-Trans-Id</li></ul>



Operation	Implementation
HEAD account	<p>Retrieves account information and statistics from a Swift account.</p> <p>The following request parameter is required:</p> <ul style="list-style-type: none"> <li>Account</li> </ul> <p>The following request header is required:</p> <ul style="list-style-type: none"> <li>X-Auth-Token</li> </ul> <p>A successful execution returns the following headers with an “HTTP/1.1 204 No Content” response:</p> <ul style="list-style-type: none"> <li>Accept-Ranges</li> <li>Content-Length</li> <li>Date</li> <li>X-Account-Bytes-Used</li> <li>X-Account-Container-Count</li> <li>X-Account-Object-Count</li> <li>X-Timestamp</li> <li>X-Trans-Id</li> </ul>

## Container operations

The following Swift API operations are performed on containers.

Operation	Implementation
DELETE container	<p>Removes an empty container from a Swift account in a StorageGRID Webscale system.</p> <p>The following request parameters are required:</p> <ul style="list-style-type: none"> <li>Account</li> <li>Container</li> </ul> <p>The following request header is required:</p> <ul style="list-style-type: none"> <li>X-Auth-Token</li> </ul> <p>A successful execution returns the following headers with an "HTTP/1.1 204 No Content" response:</p> <ul style="list-style-type: none"> <li>Content-Length</li> <li>Content-Type</li> <li>Date</li> <li>X-Trans-Id</li> </ul>

Operation	Implementation
GET container	<p>Retrieves the object list associated with the container along with container statistics and metadata in a StorageGRID Webscale system.</p> <p>The following request parameters are required:</p> <ul style="list-style-type: none"><li>• Account</li><li>• Container</li></ul> <p>The following request header is required:</p> <ul style="list-style-type: none"><li>• X-Auth-Token</li></ul> <p>The following supported request query parameters are optional:</p> <ul style="list-style-type: none"><li>• Delimiter</li><li>• End_marker</li><li>• Format</li><li>• Limit</li><li>• Marker</li><li>• Path</li><li>• Prefix</li></ul> <p>A successful execution returns the following headers with an "HTTP/1.1 200 Success" or a "HTTP/1.1 204 No Content" response:</p> <ul style="list-style-type: none"><li>• Accept-Ranges</li><li>• Content-Length</li><li>• Content-Type</li><li>• Date</li><li>• X-Container-Bytes-Used</li><li>• X-Container-Object-Count</li><li>• X-Timestamp</li><li>• X-Trans-Id</li></ul>

Operation	Implementation
HEAD container	<p>Retrieves container statistics and metadata from a StorageGRID Webscale system.</p> <p>The following request parameters are required:</p> <ul style="list-style-type: none"> <li>• Account</li> <li>• Container</li> </ul> <p>The following request header is required:</p> <ul style="list-style-type: none"> <li>• X-Auth-Token</li> </ul> <p>A successful execution returns the following headers with an "HTTP/1.1 204 No Content" response:</p> <ul style="list-style-type: none"> <li>• Accept-Ranges</li> <li>• Content-Length</li> <li>• Date</li> <li>• X-Container-Bytes-Used</li> <li>• X-Container-Object-Count</li> <li>• X-Timestamp</li> <li>• X-Trans-Id</li> </ul>
PUT container	<p>Creates a container for an account in a StorageGRID Webscale system.</p> <p>The following request parameters are required:</p> <ul style="list-style-type: none"> <li>• Account</li> <li>• Container</li> </ul> <p>The following request header is required:</p> <ul style="list-style-type: none"> <li>• X-Auth-Token</li> </ul> <p>A successful execution returns the following headers with an "HTTP/1.1 201 Created" or "HTTP/1.1 202 Accepted" (if the container already exists under this account) response:</p> <ul style="list-style-type: none"> <li>• Content-Length</li> <li>• Date</li> <li>• X-Timestamp</li> <li>• X-Trans-Id</li> </ul> <p>A container name must be unique in the StorageGRID Webscale namespace. If the container exists under another account, the following header is returned: "HTTP/1.1 409 Conflict."</p>

## Object operations

The following Swift API operations are performed on objects.

Operation	Implementation
DELETE object	<p>Deletes the metadata of an ingested object from a StorageGRID Webscale system. For the object data to be deleted, you must have a valid purge rule active.</p> <p>The following request parameters are required:</p> <ul style="list-style-type: none"><li>• Account</li><li>• Container</li><li>• Object</li></ul> <p>The following request header is required:</p> <ul style="list-style-type: none"><li>• X-Auth-Token</li></ul> <p>A successful execution returns the following response headers with an "HTTP/1.1 204 No Content" response:</p> <ul style="list-style-type: none"><li>• Content-Length</li><li>• Content-Type</li><li>• Date</li><li>• X-Trans-Id</li></ul>

Operation	Implementation
GET object	<p>Retrieves the object content and gets the object metadata from a StorageGRID Webscale system.</p> <p>The following request parameters are required:</p> <ul style="list-style-type: none"> <li>• Account</li> <li>• Container</li> <li>• Object</li> </ul> <p>The following request header is required:</p> <ul style="list-style-type: none"> <li>• X-Auth-Token</li> </ul> <p>The following request headers are optional:</p> <ul style="list-style-type: none"> <li>• Accept-Encoding</li> <li>• If-Match</li> <li>• If-Modified-Since</li> <li>• If-None-Match</li> <li>• If-Unmodified-Since</li> <li>• Range</li> </ul> <p>A successful execution returns the following headers with an "HTTP/1.1 200 OK" response:</p> <ul style="list-style-type: none"> <li>• Accept-Ranges</li> <li>• Content-Length</li> <li>• Content-Type</li> <li>• Date</li> <li>• ETag</li> <li>• Last-Modified</li> <li>• X-Timestamp</li> <li>• X-Trans-Id</li> </ul>
HEAD object	<p>Retrieves metadata and properties of an ingested object from a StorageGRID Webscale system.</p> <p>The following request parameters are required:</p> <ul style="list-style-type: none"> <li>• Account</li> <li>• Container</li> <li>• Object</li> </ul> <p>The following request header is required:</p> <ul style="list-style-type: none"> <li>• X-Auth-Token</li> </ul> <p>A successful execution returns the following headers with an "HTTP/1.1 200 OK" response:</p> <ul style="list-style-type: none"> <li>• Accept-Ranges</li> <li>• Content-Length</li> <li>• Content-Type</li> <li>• Date</li> <li>• ETag</li> <li>• Last-Modified</li> <li>• X-Timestamp</li> <li>• X-Trans-Id</li> </ul>

Operation	Implementation
PUT object	<p>Creates a new object with data and metadata, or replaces an existing object with data and metadata in a StorageGRID Webscale system.</p> <p>The following request parameters are required:</p> <ul style="list-style-type: none"> <li>Account</li> <li>Container</li> <li>Object</li> </ul> <p>The following request header is required:</p> <ul style="list-style-type: none"> <li>X-Auth-Token</li> </ul> <p>The following request headers are optional:</p> <ul style="list-style-type: none"> <li>Content-Encoding</li> <li>Content-Length</li> <li>Content-Type</li> <li>ETag</li> <li>Transfer-Encoding</li> <li>X-Object-Meta-<i>&lt;name&gt;</i> (object-related metadata)</li> </ul> <p>To record the object creation time, so that you can use the User Defined Creation Time option for the reference time in an ILM rule, you need to store the value in a user-defined header named X-Object-Meta-Creation-Time. For example: X-Object-Meta-Creation-Time=1443399726. This field is evaluated as seconds since Jan 1, 1970.</p> <p>For details, see “Reference time” in the <i>Administrator Guide</i>.</p> <ul style="list-style-type: none"> <li>X-Storage-Class:reduced_redundancy</li> </ul> <p>Specifies a single-commit ingest operation. This does not affect the information lifecycle management (ILM) policy and does not result in data being stored at lower levels of redundancy in the StorageGRID Webscale system.</p> <p>For details, see information about ILM policies in the <i>Administrator Guide</i>.</p> <p>A successful execution returns the following headers with an "HTTP/1.1 201 Created" response:</p> <ul style="list-style-type: none"> <li>Content-Length</li> <li>Content-Type</li> <li>Date</li> <li>ETag</li> <li>Last-Modified</li> <li>X-Trans-Id</li> </ul>

**Related information**

[StorageGRID Webscale 10.2 Administrator Guide](#)

## OPTIONS method

The OPTIONS request helps to check the availability of an individual Swift service. The OPTIONS request is handled by the LDR service on a Storage Node or the CLB service on the Gateway Node specified in the URL.

Operation	Implementation
OPTIONS method	<p>The OPTIONS method retrieves supported RESTful verbs for the following types of URLs: <i>info URL</i> and <i>storage URL</i> from a StorageGRID Webscale system.</p> <p>The following request parameter is required:</p> <ul style="list-style-type: none"> <li>Account</li> </ul> <p>The following request parameters are optional:</p> <ul style="list-style-type: none"> <li>Container</li> <li>Object</li> </ul> <p>A successful execution returns the following headers with an “HTTP/1.1 204 No Content” response. The OPTIONS request to the storage URL does not require that the target exists.</p> <ul style="list-style-type: none"> <li>Allow (a list of supported verbs for the given URL, for example, HEAD, GET, OPTIONS, and PUT)</li> <li>Content-Length</li> <li>Content-Type</li> <li>Date</li> <li>X-Trans-Id</li> </ul>

## Operations tracked in the audit logs

All successful storage DELETE, GET, HEAD, and PUT operations are tracked in the StorageGRID Webscale audit log.

Account operations	Container operations	Object operations
GET account	DELETE container	DELETE object
HEAD account	GET container	GET object
	HEAD container	HEAD object
	PUT container	PUT object

## Configuring tenant accounts and connections

---

Configuring StorageGRID Webscale to accept connections from Swift client applications requires creating and configuring a Swift tenant account.

### About this task

Creating and configuring tenant accounts and connections involves the following tasks:

- Create a tenant account.
- Identify IP addresses for API Gateway Nodes and Storage Nodes
- Use accurate port numbers for API Gateway Nodes and Storage Nodes

If your environment includes a form of identity federation (LDAP or AP), you should also complete the following tasks:

- Configure LDAP for identity federation.
- Edit group policies.

For details, see the *Administrator Guide*.

### Related information

[StorageGRID Webscale 10.2 Administrator Guide](#)

## Creating tenant accounts for Swift

You can create a Swift tenant account for each group that requires access to the StorageGRID Webscale system using the Swift REST API. A tenant account can be created for an organization, division, department, or any other internal or external group you want to use to define access to storage in your StorageGRID Webscale system. If you configured LDAP for this account, all groups and users in the LDAP domain can access Swift via this account.

### About this task

The Swift tenant account information is used in the authentication process. Configuring a Swift client requires one of the following sets of user credentials:

- If Identity Federation is enabled for the tenant account (for Active Directory or LDAP configurations), you should provide the username and password of the federated user from the AD or LDAP server. Alternatively, LDAP users can be referred to with their domain name, for example, X-Auth-User: `<Tenant_Account_ID>:<Username@Domain_Name>`
- For local accounts when LDAP is not configured, you should use the "swiftadmin" as the user name and the password provided during tenant account creation.

### Steps

1. Sign in to the NMS MI using the Admin account.
2. Select **Grid Management > Storage Tenants > Tenant Accounts**.
3. Click **Create**.
4. Configure the tenant account in the **Add Tenant Account** dialog box:



- a. Select **Swift** as the protocol.
- b. In the **Name** text box enter the name to display in the NMS MI.
- c. If you want to use the local Swift Administrator account, instead of or in addition to LDAP authentication, enter the password to use in the **Password** and **Confirm Password** text boxes.  
The password must be between 8 and 32 characters. You must enter a strong password to ensure the security of your StorageGRID Webscale system.
- d. Click **Save**.

## How client applications use HTTPS connections

Client applications use HTTPS connections to access and communicate with the StorageGRID Webscale system. Understanding HTTPS connections helps you understand StorageGRID Webscale requirements.

A client application can connect directly to an API Gateway Node or Storage Node to store and retrieve objects. To load balance ingests across the Storage Nodes in your grid, you can connect to an API Gateway Node, which handles the load balancing for you. Otherwise, you can connect directly to a Storage Node.

**Note:** IPv6 is supported only for client application connections through the API Gateway Node. For details about support for IPv6, see the StorageGRID Webscale Administrator Guide.

Client applications can issue `OPTIONS` HTTPS requests to the Swift port on a Storage Node, without providing Swift authentication credentials, to determine whether the LDR Service is available. You can use this request for monitoring, or to allow external load balancers to identify when a Storage Node is down.

Setting up the connection to client applications involves the following tasks:

- Creating a Swift tenant account
- Identifying IP addresses for API Gateway Nodes and Storage Nodes
- Identifying Swift port numbers for API Gateway Nodes and Storage Nodes
- Copying the system's certificate authority (CA) certificate for client applications that require server validation

For details about setting up connections, see the StorageGRID Webscale Administrator Guide.

### Related information

[\*StorageGRID Webscale 10.2 Administrator Guide\*](#)

## Identifying IP addresses for API Gateway Nodes and Storage Nodes

You need the grid node's IP address to connect API client applications to StorageGRID Webscale.

### Steps

1. In the **Grid Topology** tree, locate and expand the Storage Node or API Gateway node to which you want to connect.

The services for the selected grid node appear.

2. Select **SSM > Resources**, and then scroll to the **Network Addresses** table.

You can establish HTTPS connections from API client applications to any of the listed IP addresses.

## Port numbers on API Gateway Nodes and Storage Nodes for Swift

API Gateway Nodes and Storage Nodes are available for HTTPS connections from client applications to the StorageGRID Webscale system only on specific port numbers.

The following ports are used for Swift client applications to connect to the StorageGRID Webscale system:

Grid node	Port number
API Gateway Node (CLB Swift Port)	8083
Storage Node (LDR Swift Port)	18083

## Configuring security for the REST API

---

You need to understand the security measures implemented for the REST API and how to secure your system.

### How the StorageGRID Webscale system implements security for the REST API

The StorageGRID Webscale system employs the use of Transport Layer Security (TLS) connection security, server authentication, client authentication, and client authorization. When considering security issues, you might find it helpful to understand how the StorageGRID Webscale system implements security, authentication, and authorization for the S3 or Swift REST API.

The StorageGRID Webscale system accepts HTTPS commands submitted over a network connection that uses TLS to provide connection security, application authentication and, optionally, transport encryption. Commands that do not use TLS are rejected. If an object is encrypted when it is ingested, it stays encrypted for the lifetime of the object in the StorageGRID Webscale system.

TLS enables the exchange of certificates as entity credentials and allows a negotiation that can use hashing and encryption algorithms.

When a StorageGRID Webscale system is installed, a certificate authority (CA) certificate is generated, as well as server certificates for each Storage Node. These server certificates are all signed by the grid CA. You need to configure client applications to trust this grid CA certificate. When a client application connects to any Storage Node using TLS, the application can authenticate the Storage Node by verifying that the server certificate presented by the Storage Node is signed by the trusted grid CA.

Alternatively, you can choose to supply a single, custom server certificate that should be used on all Storage Nodes rather than the generated ones. The custom server certificate must be signed by a CA selected by the administrator. The server authentication process by the client application is the same, but in this instance with a different trusted CA.

For details about configuring server certificates, see the *Administrator Guide*.

The following table shows how security issues are implemented for S3 and Swift API:

Security issue	Implementation for REST API
Connection security	TLS
Server authentication	X.509 server certificate signed by grid CA or custom server certificate supplied by administrator
Client authentication	<ul style="list-style-type: none"> <li>S3: S3 account (access key ID and secret access key)</li> <li>Swift: Swift account (credentials of user name and password)</li> </ul>
Client authorization	<ul style="list-style-type: none"> <li>S3: Bucket ownership and all applicable access control policies</li> <li>Swift: Account admin role access</li> </ul>

#### Related information

[StorageGRID Webscale 10.2 Administrator Guide](#)

## Configuring a custom server certificate

If you want to use a single server certificate for all grid nodes in your StorageGRID Webscale system, you need to configure a custom server certificate.

### About this task

When a client application establishes a Transport Layer Security (TLS) session to the StorageGRID Webscale system, the target LDR service on the Storage Node sends a server certificate to the client application. By default, each Storage Node identifies itself by using a separate certificate that is signed by the system Certificate Authority (CA). Rather than use separate server certificates, you can choose to use a single server certificate supplied by you for all Storage Nodes. This provides flexibility in enabling support for certificate hostname verification.

Only RSA custom server certificates are supported.

The certificate and private key should be entered in PEM format.

You can choose to use the wildcard certificate format: for example, \*.storagegrid.mycompany.com. In this case, API Gateway Nodes and Storage Nodes must have DNS entries that map their IP addresses to host names that match the wildcards: for example, dc1-gw1.storagegrid.mycompany.com and dc2-s3.storagegrid.mycompany.com. Client applications are then configured to connect to the system using these DNS names, which enables host name verification.


### Steps

1. In the NMS MI, select **Grid Management > Grid Configuration > Configuration > Main**.
2. In the Custom Server Certificate box inside the **API Server Certificates** section, copy and paste the server certificate, including the -----BEGIN CERTIFICATE----- and the -----END CERTIFICATE----- encapsulation boundaries.

Overview


Configuration

Main




**Configuration: Grid Configuration**  
Updated: 2014-05-14 14:40:28 PDT

---


**API Server Certificates**


API service endpoints (LDR services) are secured and identified by X.509 server certificates. By default, every LDR service is issued a certificate signed by the grid CA. These CA signed certificates can be replaced by a single common custom server certificate and corresponding private key.

Custom Server Certificate	MFVEndfP1hzS0m80ukcmcAAN4VKcQbwmh0UfAA9RsEiCgOKyp8yc9lh6ZbwCw== -----END CERTIFICATE-----
Custom Private Key	IdEB6T+pp1k69MGRXeZklVC42uZQOBM= -----END RSA PRIVATE KEY-----

**Grid Options**


Grid Language	United States - English
Stored Object Compression	Disabled
Stored Object Encryption	Disabled
Stored Object Hashing	SHA-256
Disable Client Delete	Disabled
Security Partitions	Disabled
Network Transfer Encryption	AES256-SHA

**Grid Specification File**


Click the export button to view the Grid Specification File.

- In the Custom Private Key box, copy and paste the corresponding private key, including -----BEGIN RSA PRIVATE KEY----- and the -----END RSA PRIVATE KEY-----.
- This must be an unencrypted private key.
- Click **Apply Changes**.
- The private key becomes obscured.
- Click **Overview** to see the custom certificate on the **Overview** page.
- Note:** The CA Certificate box on the Overview page displays the default generated server certificate.
- If a custom server certificate is issued by one or more intermediate CAs, you must also enter the certificates of all intermediate CAs within **Grid Management > HTTP Management > Certificates > Certificate Authorities > Configuration > Main**.
- For details about HTTP management, see the *Administrator Guide*.

#### After you finish

If you configured a custom server certificate, then clients should verify using the root CA certificate that issued the custom server certificate. However, if you use the default certificate, then client applications should verify connections using the system certificate.

#### Related information

[StorageGRID Webscale 10.2 Administrator Guide](#)

## Reverting a custom server certificate to the default certificate

You can change from using your custom server certificate back to using the default, automatically generated certificate. You might want to revert to the default certificate if, for example, the custom certificate has expired.

### Steps

1. In the NMS MI, select **Grid Management > Grid Configuration > Configuration > Main**.
2. In the API Server Certificates section, delete the text from the Custom Server Certificate box.
3. Delete the text from the Custom Private Key box.
4. Click **Apply Changes**.
5. Click **Overview** to see the default certificate on the **Overview** page.

### After you finish

You must reconfigure your client applications to use the default system CA certificate.

## Copying the StorageGRID Webscale system's CA certificate

You can copy the StorageGRID Webscale system's certificate authority (CA) certificate from the Network Management System (NMS) Management Interface (MI) for client applications that require server verification. If a custom server certificate has been configured, then client applications should verify the server using the root CA certificate that issues the custom server certificate, rather than copy the CA certificate from the NMS MI.

### Steps


1. In the NMS MI, select **Grid Management > Grid Configuration > Overview > Main**.
2. Under **API Server Certificates**, expand **CA Certificate**.
3. Select the CA certificate.

Include the “-----BEGIN CERTIFICATE-----” and the “-----END CERTIFICATE-----” in your selection.

Overview

Configuration

Main



**Overview: Grid Configuration**  
 Updated: 2015-04-15 15:38:50 PDT

---

**Grid Information**

Grid ID:	401698
Configured:	2015-04-09 20:17:12 PDT
Vendor:	NetApp Inc.
Software Suite Interoperability Version:	10.0.0

---

**API Server Certificates**

API service endpoints (LDR services) are secured and identified by X.509 server certificates. By default, every LDR service is issued a certificate signed by the grid CA. These CA signed certificates can be replaced by a single common custom server certificate and corresponding private key.

CA Certificate:

☒ CN=GPT, OU=NetApp StorageGRID, O=NetApp Inc., L=Sunnyvale, ST=California, C=US

```

-----BEGIN CERTIFICATE-----
MIIEETjCCAzagAwIBAgIJALdW/01WU1oUMA0GCSqGSIb3DQEBCwUAMHcxZzhhGUX
BAYTA1VTMRMwEQYDVQIEwPDYXpZm9ybmlhMRIwEAYDVQQHEw1TdW5ueXZhbGUX
FDASBgNVBAoTC051dEFwcCBJbmMuMRswGQYDVQQLExJOZXRBCkAgU3RvcnFnZUdS
SUQxDDAKBgNVBAMTA0dQVDAeFw0xNTA0MTAwMzE0MDJaFw0zODAxMTgwMzE0MDJa
MHcxZzhhGUXBAYTA1VTMRMwEQYDVQIEwPDYXpZm9ybmlhMRIwEAYDVQQHEw1T
dW5ueXZhbGUXFDASBgNVBAoTC051dEFwcCBJbmMuMRswGQYDVQQLExJOZXRBCkAg
U3RvcnFnZUdSSUQxDDAKBgNVBAMTA0dQVDAeFw0xNTA0MTAwMzE0MDJaFw0zODAx
MTgwMzE0MDJaADCCAQoCggEBANKmFruahDQbE0RodeZYnjQHmNHwGWznn4p9iDIR1KxpYapvyXhk
73SAnagnD7uTGd0x4+b4ehJ/wi/tAOsrLA2ypMSQCW14PcA2gc7fr3HAMCOboavT
o/L72U/h9FwvB16mAsN0Aun5uvyYWF5D75fANX7nSy/9Qw5gtvtxsnHWV4IGAYH2
xDlhNkanBs6qJ3ykZonDGZb5pj11Iicj5duTk7YspdaeR3zbtmVvOfUQgds1biT
3FxxZxMGBzbwRR/7hJZZGaI33EtOZFH1n+3nGRohpBaEGijz5ieMoTsHwB01eTrE
GRhTQ8508UhdJfjAtSu7uIrtY2YGzIDuj/ECawEAAaOB3DCB2TadBgNVHQ4EFgQU
gVCvArCd9jpYK10HX9J3WtelF2EwgakGA1UdIwSBTCBnoAUgVVCvArCd9jpYK10H
X9J3WtelF2Ghe6R5MHcxZzhhGUXBAYTA1VTMRMwEQYDVQIEwPDYXpZm9ybmlh
MRIwEAYDVQQHEw1TdW5ueXZhbGUXFDASBgNVBAoTC051dEFwcCBJbmMuMRswGQYD
VQQLExJOZXRBCkAgU3RvcnFnZUdSSUQxDDAKBgNVBAMTA0dQVDAeFw0xNTA0MTAw
MzE0MDJaFw0zODAxMTgwMzE0MDJaMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEL
BQADggEBAFiuTqXrgNYzK1G8sp30
yd6SNQBgcoxOhJWfWITh3V0tNR5vcYY22IDx8B8LoIt+ykBS4aWxhJ9aGS7MUs/bT
oHE8x7iW1Vkf13wsJXDXnFHPjUWK82vtPPEHA/LUmQbJDLZYUzdMB9tPdqyW04MY
8prEdAeP3gkAv1lvmMJNEAphwCI70Sthcj46pFntRznDGHXaiOio89UGcmfXW6e6
zdM2mOZx1WgzG9p81oc7Gnlz585AhFixEI5Woy28cImnFhKZmks222Y11GSCkh
fnKRJw1rCugrDmVnbh08GkBiYDPx6GxpMtQbUaQVdH2pVdghc5B13VpEszbGw4qj
KhY=
-----END CERTIFICATE-----

```

Custom Server Certificate:

Not configured

- Right-click the selected certificate, and then select **Copy**.

## How client applications use certificates for security with REST APIs

When a client application establishes a TLS session to the StorageGRID Webscale system, the system sends a server certificate to the client application for verification to ensure that the HTTPS connection is secure.

The client application loads the grid CA certificate and uses it to verify that the client application is communicating with the expected StorageGRID Webscale system. This process protects against man-in-the-middle and impersonation attacks.

## Supported hashing and encryption algorithms for TLS libraries

Client applications use the HTTPS protocol to communicate with the StorageGRID Webscale system over a network connection that uses Transport Layer Security (TLS). The StorageGRID Webscale supports a limited set of hashing and encryption algorithms from the TLS libraries that client

applications can use when establishing a TLS session. When you are setting up the communication processes, it is important for you to know which security algorithms the system uses.

The StorageGRID Webscale system supports the following cipher suite security algorithms:

- AES128-SHA
- AES256-SHA
- NULL-SHA
- NULL-MD5

Based on system measurements and general security domain knowledge, AES128-SHA and AES256-SHA provide reasonable security without requiring inordinate amounts of computational resources. The choice between AES128-SHA and AES256-SHA depends on the client application requirements that balance performance with encryption security.

**Note:** You should use one of the NULL ciphers if encryption is not required and you want to eliminate the overhead associated with encryption. The client application must explicitly request the NULL cipher.



## Testing your connection in the Swift API configuration

---

You can use the Swift CLI to test your connection to the StorageGRID Webscale system and to verify that you can read and write objects to the system.

### Before you begin

- You must have downloaded and installed *python-swiftclient*, the Swift command-line client, at <https://swiftstack.com/docs/integration/python-swiftclient.html>.
- You must have created a Swift tenant account in the NMS MI.

### About this task

If you have not configured security as described in configuring security information, then you must add the `--insecure` flag to each of these commands.

### Steps

1. Query the info URL for your StorageGRID Webscale Swift deployment:

```
swift
-U <Tenant_Account_ID:User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/info
capabilities
```

This is sufficient to test that your Swift deployment is functional. To further test account configuration by storing an object, continue with the additional steps.

2. Put an object in the container:

```
touch test_object
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
upload test_container test_object
--object-name test_object
```

3. Get the container to verify the object:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. Delete the object:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. Delete the container:

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN / IP>:<Port>/auth/v1.0
delete test_container
```

**Related tasks**

[\*Creating tenant accounts for Swift\*](#) on page 16

## Monitoring and auditing operations

---

You can monitor the health of your client application connections to the StorageGRID Webscale system by viewing summary attributes that list transaction counts for all LDR services, or you can view the transactions for a specific LDR service. Also, you can use audit messages to monitor the operations and transactions of the StorageGRID Webscale system.

### Steps

1. [Viewing HTTPS transactions for Swift objects](#) on page 27  
You can view the number of successful and failed attempts by client applications to read, write, and modify Swift objects in the StorageGRID Webscale system. You can view a summary of all transactions for all LDR services, or you can view the transactions for a specific LDR service. You might want to do this to evaluate the health of the system.
2. [Viewing information about data objects](#) on page 28  
You can use an object ID in the NMS MI to view information about the data object in the StorageGRID Webscale system. You can check on the current location of the object and obtain any metadata associated with the object.
3. [Accessing and reviewing audit logs](#) on page 28  
The StorageGRID Webscale system securely and reliably transports audit messages from each service within the StorageGRID Webscale system to one or more audit repositories. API-specific (SGAPI, CDMI, S3, and Swift) audit messages provide critical security, operations, and performance monitoring data that can help you evaluate the health of your system.

## Viewing HTTPS transactions for Swift objects

You can view the number of successful and failed attempts by client applications to read, write, and modify Swift objects in the StorageGRID Webscale system. You can view a summary of all transactions for all LDR services, or you can view the transactions for a specific LDR service. You might want to do this to evaluate the health of the system.

### Steps

1. In the NMS MI, select **Grid Topology** > *<grid\_name>* > **Overview** > **Main**, and then view the **API Operations** area.

The grid name is the top-level entry in the Grid Topology tree. The API Operations area displays a summary of information from all of the LDR services that support Swift client applications.

Overview

Alarms

Reports

Configuration

Main

Tasks

Future ILM Activity

Time Period	Number of Objects
Within 24Hrs	0
Beyond 24Hrs	0

API Operations

CDMI Operations - Rate:	0 Operations/s	
CDMI Operations - Successful:	0	
CDMI Operations - Failed:	0	
CDMI - Received Bytes:	0 B	
CDMI - Transmitted Bytes:	0 B	
S3 Operations - Rate:	0 Operations/s	
S3 Operations - Successful:	0	
S3 Operations - Failed:	0	
S3 Operations - Unauthorized:	0	
S3 - Received Bytes:	0 B	
S3 - Transmitted Bytes:	0 B	
Swift Operations - Rate:	0 Operations/s	
Swift Operations - Successful:	79	
Swift Operations - Failed:	3	
Swift Operations - Unauthorized:	16	
Swift - Received Bytes:	2.62 KB	
Swift - Transmitted Bytes:	0 B	

2. Select **Grid Topology** > **<grid\_ node>** > **LDR** > **Swift** > **Overview** > **Main** to view information for individual LDR services.

## Viewing information about data objects

You can use an object ID in the NMS MI to view information about the data object in the StorageGRID Webscale system. You can check on the current location of the object and obtain any metadata associated with the object.

### Steps

1. Obtain the object ID from the client application.
2. In the NMS MI, select **Grid Topology** > **Admin Node** > **CMN** > **Object Lookup**.
3. Click **Configuration**.
4. In the **Object Identifier** box, enter one of the following object IDs, and click **Apply Changes**:
  - CBID (content block identifier)
  - UUID (universally unique identifier)
  - Object ID
  - Container/Object\_Key

**Note:** If you enter an invalid object ID, an error message appears.

5. Click **Overview** to review the results.

## Accessing and reviewing audit logs

The StorageGRID Webscale system securely and reliably transports audit messages from each service within the StorageGRID Webscale system to one or more audit repositories. API-specific

(SGAPI, CDMI, S3, and Swift) audit messages provide critical security, operations, and performance monitoring data that can help you evaluate the health of your system.

**About this task**

The StorageGRID Webscale system compresses audit logs after one day and renames them using the format `YYYY-MM-DD.txt.gz` (where the original date is preserved).

**Steps**

1. Log in to the server using the user name and password as recorded in the `Passwords.txt` file.
2. Access the audit log directory through a command line of the server that hosts the AMS service.
3. Go to the `/var/local/audit/export/` directory.
4. View the `audit.log` file.

## Copyright information

---

Copyright © 1994–2015 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.

**RESTRICTED RIGHTS LEGEND:** Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## Trademark information

---

NetApp, the NetApp logo, Go Further, Faster, AltaVault, ASUP, AutoSupport, Campaign Express, Cloud ONTAP, Clustered Data ONTAP, Customer Fitness, Data ONTAP, DataMotion, Fitness, Flash Accel, Flash Cache, Flash Pool, FlashRay, FlexArray, FlexCache, FlexClone, FlexPod, FlexScale, FlexShare, FlexVol, FPolicy, GetSuccessful, LockVault, Manage ONTAP, Mars, MetroCluster, MultiStore, NetApp Insight, OnCommand, ONTAP, ONTAPI, RAID DP, RAID-TEC, SANtricity, SecureShare, Simplicity, Simulate ONTAP, Snap Creator, SnapCenter, SnapCopy, SnapDrive, SnapIntegrator, SnapLock, SnapManager, SnapMirror, SnapMover, SnapProtect, SnapRestore, Snapshot, SnapValidator, SnapVault, StorageGRID, Tech OnTap, Unbound Cloud, and WAFL and other names are trademarks or registered trademarks of NetApp, Inc., in the United States, and/or other countries. All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such. A current list of NetApp trademarks is available on the web at <http://www.netapp.com/us/legal/netapptmlist.aspx>.

## How to send comments about documentation and receive update notifications

---

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email to [doccomments@netapp.com](mailto:doccomments@netapp.com). To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277



# Index

## A

- account operations
  - how implemented [8](#)
- algorithms
  - encryption [23](#)
  - hash [23](#)
  - supported by TLS [23](#)
- API
  - configuring security for [19](#)
  - OpenStack Swift version supported [4](#)
- API Gateway Nodes
  - IP address of [17](#)
  - IP addresses on CLB service [17](#)
  - port numbers for Swift API [18](#)
- API operations
  - account [8](#)
  - container [9](#)
  - object [12](#)
- applications
  - use of HTTPS connections [17](#)
  - viewing HTTPS transactions for Swift objects [27](#)
- audit logs
  - operations tracked [15](#)
  - reviewing [28](#)
  - using to monitor operations [27](#)
- auth URL
  - overview [5](#)
- authentication
  - HTTP connections [19](#)

## C

- certificate authority (CA) certificates
  - configuring custom [20](#)
  - copying for StorageGRID Webscale system [22](#)
  - how client applications use for security with REST APIs [23](#)
  - reverting to default [22](#)
- CLB service
  - IP addresses [17](#)
  - OPTIONS request [15](#)
  - port numbers for Swift [18](#)
  - Swift API endpoints [5](#)
- client applications
  - how certificates are used for security with REST APIs [23](#)
  - HTTPS connections used to communicate with StorageGRID Webscale [17](#)
  - HTTPS connections used with StorageGRID Webscale [17](#)
  - viewing HTTPS transactions for Swift objects [27](#)
- comments
  - how to send feedback about documentation [32](#)
- connecting
  - configuring custom server certificates [20](#)
  - how client applications use to communicate with StorageGRID Webscale [17](#)
  - reverting to default server certificate [22](#)

- security and TLS in S3 or Swift API [19](#)
- tenant configuration overview [16](#)
- testing [25](#)

- container
  - operations [9](#)
- credentials
  - for Active Directory or LDAP [16](#)
  - without LDAP [16](#)

## D

- documentation
  - how to receive automatic notification of changes to [32](#)
  - how to send feedback about [32](#)

## E

- encryption algorithms
  - supported by TLS [23](#)

## F

- feedback
  - how to send comments about documentation [32](#)

## G

- grid nodes
  - IP addresses for [17](#)

## H

- hash algorithms
  - supported by TLS [23](#)
- HTTPS connections
  - copying CA certificates [22](#)
  - how client applications use certificates for security with REST APIs [23](#)
  - how client applications use to access and communicate with StorageGRID systems [17](#)
  - IP address for grid nodes [17](#)
  - viewing transactions by client applications [27](#)

## I

- info URL
  - OPTIONS method with [15](#)
  - overview [5](#)
- information
  - how to send feedback about improving documentation [32](#)
- IP addresses
  - for API Gateway Nodes [17](#)
  - for Storage Nodes [17](#)

**L**

## LDR service

- IP addresses [17](#)
- OPTIONS request [15](#)
- port numbers for Swift [18](#)
- Swift API endpoints [5](#)
- viewing HTTPS transactions [27](#)

## logs

- audit [15](#)
- reviewing audit [28](#)

**M**

## metadata

- viewing for objects [28](#)

**O**

## object storage

- enabled by support for Swift OpenStack API [4](#)

## objects

- operations [12](#)
- viewing HTTPS transactions for [27](#)
- viewing information about [28](#)

## OpenStack Swift API

- version supported [4](#)

## operations

- accounts [8](#)
- container [9](#)
- error responses [5](#), [7](#)
- monitoring [27](#)
- objects [12](#)
- overview [5](#)
- tracked in audit log [15](#)

## OPTIONS method

- described [15](#)

**P**

## port numbers

- for API Gateway Nodes for Swift API [18](#)
- for Storage Nodes for Swift API [18](#)

**R**

## REST API

- configuring security for S3 [19](#)
- configuring security for Swift [19](#)

**S**

## security

- configuring for REST API [19](#)
- how client applications use certificates for with REST APIs [23](#)
- how client applications use certificates with S3 [23](#)
- how client applications use certificates with Swift [23](#)
- StorageGRID Webscale CA certificate [22](#)

Transport Layer Security [19](#)

## server authentication

- S3 or Swift [19](#)

## server certificates

- configuring custom [20](#)
- copying [22](#)
- how client applications use for security with REST APIs [23](#)
- reverting custom [22](#)

## Storage Nodes

- configuring custom server certificates [20](#)
- IP address of [17](#)
- IP addresses on LDR service [17](#)
- port numbers for Swift API [18](#)

## storage URL

- OPTIONS method with [15](#)
- overview [5](#)

## StorageGRID Webscale

- copying CA certificates [22](#)
- HTTPS connections with client applications [17](#)
- port numbers for Swift [18](#)
- security for REST API [19](#)
- Swift API account operations [8](#)
- Swift API OPTIONS request [15](#)
- testing connection with Swift API [25](#)

## suggestions

- how to send feedback about documentation [32](#)

## Swift API operations

- account [8](#)
- container [9](#)
- object [12](#)

## Swift REST API

- changes to support of [4](#)
- creating tenant accounts [16](#)
- how implemented [4](#)
- testing configuration [25](#)
- version supported [4](#)
- viewing HTTPS transactions for [27](#)

**T**

## tenant accounts

- configuring [16](#)
- creating for Swift [16](#)

## TLS

- how client applications use certificates for security with REST APIs [23](#)
- security in S3 or Swift API [19](#)
- supported hashing algorithms [23](#)

## Transport Layer Security

- .See TLS

## troubleshooting

- error responses to operations [5](#), [7](#)
- using audit logs [28](#)

## twitter

- how to receive automatic notification of documentation changes [32](#)

**U**URL types [5](#)