Configuring server certificates

StorageGRID 11.5

NetApp
January 04, 2024

Table of Contents

Configuring server certificates

You can customize the server certificates used by the StorageGRID system.

The StorageGRID system uses security certificates for multiple distinct purposes:

- Management Interface Server Certificates: Used to secure access to the Grid Manager, the Tenant Manager, the Grid Management API, and the Tenant Management API.
- Storage API Server Certificates: Used to secure access to the Storage Nodes and Gateway Nodes, which API client applications use to upload and download object data.

You can use the default certificates created during installation, or you can replace either, or both, of these default types of certificates with your own custom certificates.

Supported types of custom server certificate

The StorageGRID system supports custom server certificates encrypted with RSA or ECDSA (Elliptic Curve Digital Signature Algorithm).

For more information on how StorageGRID secures client connections for the REST API, see the S3 or Swift implementation guides.

Certificates for load balancer endpoints

StorageGRID manages the certificates used for load balancer endpoints separately. To configure load balancer certificates, see the instructions for configuring load balancer endpoints.

Related information

Use S3

Use Swift

Configuring load balancer endpoints

Configuring a custom server certificate for the Grid Manager and the Tenant Manager

You can replace the default StorageGRID server certificate with a single custom server certificate that allows users to access the Grid Manager and the Tenant Manager without encountering security warnings.

About this task

By default, every Admin Node 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.

Because a single custom server certificate is used for all Admin Nodes, you must specify the certificate as a wildcard or multi-domain certificate if clients need to verify the hostname when connecting to the Grid Manager and Tenant Manager. Define the custom certificate such that it matches all Admin Nodes in the grid.

You need to complete configuration on the server, and depending on the root Certificate Authority (CA) you are

using, users might also need to install the root CA certificate in the web browser they will use to access the Grid Manager and the Tenant Manager.

> To ensure that operations are not disrupted by a failed server certificate, the **Expiration of server certificate for Management Interface** alert and the legacy Management Interface Certificate Expiry (MCEP) alarm are both triggered when this server certificate is about to expire. As required, you can view the number of days until the current service certificate expires by selecting **Support** > **Tools** > **Grid Topology**. Then, select ***primary Admin Node*** > **CMN** > **Resources**.

> If you are accessing the Grid Manager or Tenant Manager using a domain name instead of an IP address, the browser shows a certificate error without an option to bypass if either of the following occurs:
>
> - Your custom management interface server certificate expires.
> - You revert from a custom management interface server certificate to the default server certificate.

Steps

1. Select **Configuration** > **Network Settings** > **Server Certificates**.
2. In the Management Interface Server Certificate section, click **Install Custom Certificate**.
3. Upload the required server certificate files:
   - **Server Certificate**: The custom server certificate file (`.crt`).
   - **Server Certificate Private Key**: The custom server certificate private key file (`.key`).

     > EC private keys must be 224 bits or larger. RSA private keys must be 2048 bits or larger.

   - **CA Bundle**: A single file containing the certificates from each intermediate issuing Certificate Authority (CA). The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.
4. Click **Save**.

   The custom server certificates are used for all subsequent new client connections.

   Select a tab to display detailed information about the default StorageGRID server certificate or a CA signed certificate that was uploaded.

   > After uploading a new certificate, allow up to one day for any related certificate expiration alerts (or legacy alarms) to clear.

5. Refresh the page to ensure the web browser is updated.

Restoring the default server certificates for the Grid Manager and the Tenant Manager

You can revert to using the default server certificates for the Grid Manager and the Tenant Manager.

Steps

1. Select **Configuration** > **Network Settings** > **Server Certificates**.
2. In the Manage Interface Server Certificate section, click **Use Default Certificates**.
3. Click **OK** in the confirmation dialog box.

   When you restore the default server certificates, the custom server certificate files you configured are deleted and cannot be recovered from the system. The default server certificates are used for all subsequent new client connections.

4. Refresh the page to ensure the web browser is updated.

Configuring a custom server certificate for connections to the Storage Node or the CLB service

You can replace the server certificate that is used for S3 or Swift client connections to the Storage Node or to the CLB service (deprecated) on Gateway Node. The replacement custom server certificate is specific to your organization.

About this task

By default, every Storage Node is issued a X.509 server certificate signed by the grid CA. These CA signed certificates can be replaced by a single common custom server certificate and corresponding private key.

A single custom server certificate is used for all Storage Nodes, so you must specify the certificate as a wildcard or multi-domain certificate if clients need to verify the hostname when connecting to the storage endpoint. Define the custom certificate such that it matches all Storage Nodes in the grid.

After completing configuration on the server, users might also need to install the root CA certificate in the S3 or Swift API client they will use to access the system, depending on the root Certificate Authority (CA) you are using.

> To ensure that operations are not disrupted by a failed server certificate, the **Expiration of server certificate for Storage API Endpoints** alert and the legacy Storage API Service Endpoints Certificate Expiry (SCEP) alarm are both triggered when the root server certificate is about to expire. As required, you can view the number of days until the current service certificate expires by selecting **Support** > **Tools** > **Grid Topology**. Then, select ***primary Admin Node*** > **CMN** > **Resources**.

The custom certificates are only used if clients connect to StorageGRID using the deprecated CLB service on Gateway Nodes, or if they connect directly to Storage Nodes. S3 or Swift clients that connect to StorageGRID using the Load Balancer service on Admin Nodes or Gateway Nodes use the certificate configured for the load balancer endpoint.

> The **Expiration of load balancer endpoint certificate** alert is triggered for load balancer endpoints that will expire soon.

Steps

1. Select **Configuration** > **Network Settings** > **Server Certificates**.
2. In the Object Storage API Service Endpoints Server Certificate section, click **Install Custom Certificate**.
3. Upload the required server certificate files:

- **Server Certificate**: The custom server certificate file (`.crt`).
- **Server Certificate Private Key**: The custom server certificate private key file (`.key`).

  EC private keys must be 224 bits or larger. RSA private keys must be 2048 bits or larger.

- **CA Bundle**: A single file containing the certificates from each intermediate issuing Certificate Authority (CA). The file should contain each of the PEM-encoded CA certificate files, concatenated in certificate chain order.

4. Click **Save**.

   The custom server certificate is used for all subsequent new API client connections.

   Select a tab to display detailed information about the default StorageGRID server certificate or a CA signed certificate that was uploaded.

   After uploading a new certificate, allow up to one day for any related certificate expiration alerts (or legacy alarms) to clear.

5. Refresh the page to ensure the web browser is updated.

Related information

Use S3

Use Swift

Configuring S3 API endpoint domain names

Restoring the default server certificates for the S3 and Swift REST API endpoints

You can revert to using the default server certificates for the S3 and Swift REST API endpoints.

Steps

1. Select **Configuration** > **Network Settings** > **Server Certificates**.
2. In the Object Storage API Service Endpoints Server Certificate section, click **Use Default Certificates**.
3. Click **OK** in the confirmation dialog box.

   When you restore the default server certificates for the object storage API endpoints, the custom server certificate files you configured are deleted and cannot be recovered from the system. The default server certificates are used for all subsequent new API client connections.

4. Refresh the page to ensure the web browser is updated.

Copying the StorageGRID system's CA certificate

StorageGRID uses an internal Certificate Authority (CA) to secure internal traffic. This certificate does not change if you upload your own certificates.

What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have specific access permissions.

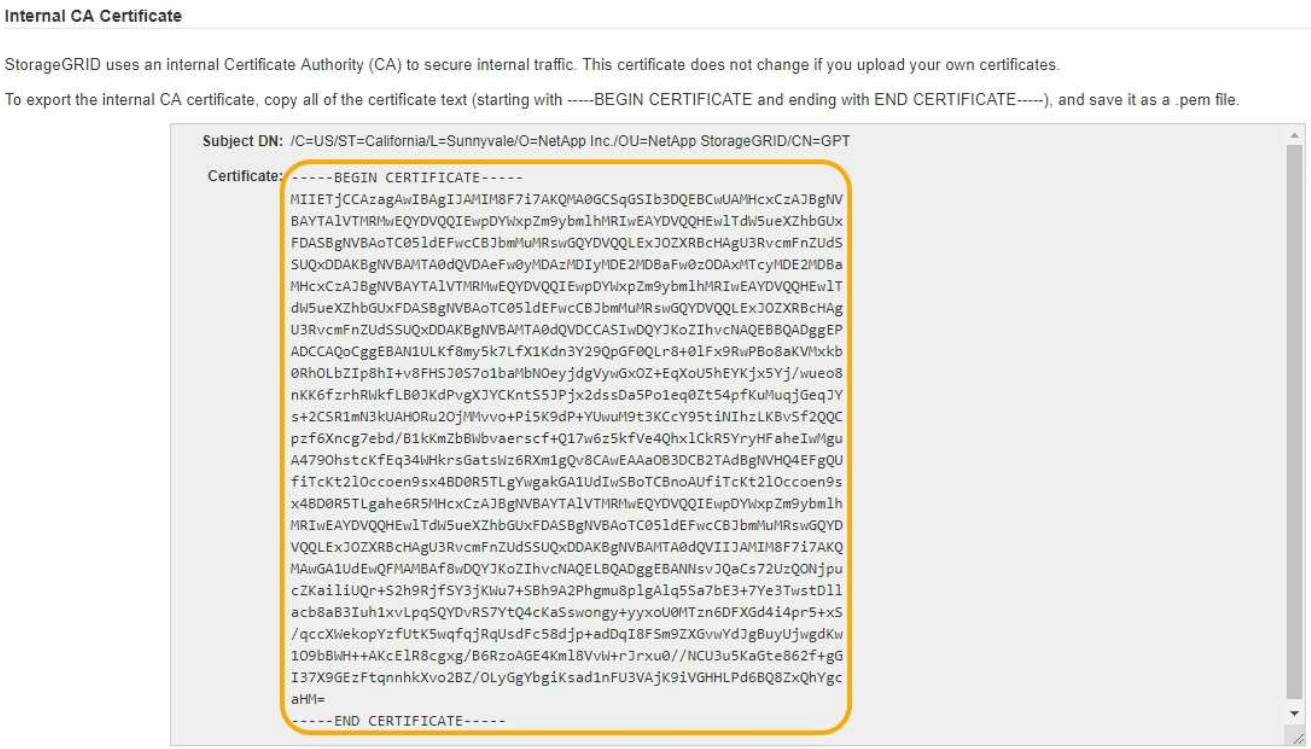
About this task

If a custom server certificate has been configured, client applications should verify the server using the custom server certificate. They should not copy the CA certificate from the StorageGRID system.

Steps

1. Select **Configuration** > **Network Settings** > **Server Certificates**.
2. In the **Internal CA Certificate** section, select all of the certificate text.

   You must include `-----BEGIN CERTIFICATE-----` and `-----END CERTIFICATE-----` in your selection.



3. Right-click the selected text, and select **Copy**.
4. Paste the copied certificate into a text editor.
5. Save the file with the extension `.pem`.

   For example: `storagegrid_certificate.pem`

Configuring StorageGRID certificates for FabricPool

For S3 clients that perform strict hostname validation and do not support disabling strict hostname validation, such as ONTAP clients using FabricPool, you can generate or upload a server certificate when you configure the load balancer endpoint.

What you'll need

- You must have specific access permissions.
- You must be signed in to the Grid Manager using a supported browser.

About this task

When you create a load balancer endpoint, you can generate a self-signed server certificate or upload a certificate that is signed by a known Certificate Authority (CA). In production environments, you should use a certificate that is signed by a known CA. Certificates signed by a CA can be rotated non-disruptively. They are also more secure because they provide better protection against man-in-the-middle attacks.

The following steps provide general guidelines for S3 clients that use FabricPool. For more detailed information and procedures, see the instructions for configuring StorageGRID for FabricPool.

> The separate Connection Load Balancer (CLB) service on Gateway Nodes is deprecated and no longer recommended for use with FabricPool.

Steps

1. Optionally, configure a high availability (HA) group for FabricPool to use.
2. Create an S3 load balancer endpoint for FabricPool to use.

   When you create an HTTPS load balancer endpoint, you are prompted to upload your server certificate, certificate private key, and CA bundle.

3. Attach StorageGRID as a cloud tier in ONTAP.

   Specify the load balancer endpoint port and the fully qualified domain name used in the CA certificate you uploaded. Then, provide the CA certificate.

   > If an intermediate CA issued the StorageGRID certificate, you must provide the intermediate CA certificate. If the StorageGRID certificate was issued directly by the Root CA, you must provide the Root CA certificate.

Related information

Configure StorageGRID for FabricPool

Generating a self-signed server certificate for the management interface

You can use a script to generate a self-signed server certificate for management API clients that require strict hostname validation.

What you'll need

- You must have specific access permissions.
- You must have the `Passwords.txt` file.

About this task

In production environments, you should use a certificate that is signed by a known Certificate Authority (CA). Certificates signed by a CA can be rotated non-disruptively. They are also more secure because they provide better protection against man-in-the-middle attacks.

Steps

1. Obtain the fully qualified domain name (FQDN) of each Admin Node.
2. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_Node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

   When you are logged in as root, the prompt changes from `$` to `#`.
3. Configure StorageGRID with a new self-signed certificate.

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - For `--domains`, use wildcards to represent the fully qualified domain names of all Admin Nodes. For example, `*.ui.storagegrid.example.com` uses the * wildcard to represent `admin1.ui.storagegrid.example.com` and `admin2.ui.storagegrid.example.com`.
   - Set `--type` to `management` to configure the certificate used by Grid Manager and Tenant Manager.
   - By default, generated certificates are valid for one year (365 days) and must be recreated before they expire. You can use the `--days` argument to override the default validity period.

   > ⓘ A certificate's validity period begins when `make-certificate` is run. You must ensure the management API client is synchronized to the same time source as StorageGRID; otherwise, the client might reject the certificate.

   ```
   $ sudo make-certificate --domains *.ui.storagegrid.example.com --type
   management --days 365
   ```

   The resulting output contains the public certificate needed by your management API client.
4. Select and copy the certificate.

   Include the BEGIN and the END tags in your selection.
5. Log out of the command shell. `$ exit`
6. Confirm the certificate was configured:
   a. Access the Grid Manager.
   b. Select **Configuration** > **Server Certificates** > **Management Interface Server Certificate**.
7. Configure your management API client to use the public certificate you copied. Include the BEGIN and END tags.

Copyright information

Trademark information