GroupWise Mobility Service 2014 R2 Security Enhancements Quick Start

August 2016

GroupWise Mobility Service 2014 R2 has enhanced the security options available to administrators. This document takes you through the security enhancements and how they can secure your system.

Security Enhancements

The following are the enhancements that have been made to GroupWise Mobility Service to make communication more secure:

- SSL Requirements
- SSL Recommendations (Optional)
- GMSsslCheck
- Certificate Verification

SSL Requirements

- Before upgrading or installing GMS 2014 R2, all POAs need to either have SSL enabled or disabled. SSL failover is no longer available.
- POA certificates should be issued to the DNS name of the POA server.

SSL Recommendations (Optional)

- If you have run against a POA that didn't have SSL enabled in the past, create a new GroupWise trusted application for GMS before enabling SSL.
- Consolidate to one CA for your GroupWise system.
- Use a public CA for your GroupWise system.
- Use a wildcard certificate for all of your POAs.

GMSsslCheck

A new tool has been created because of the SSL changes to ensure that all GroupWise POAs are correctly setup for the SSL settings you have set in GMS.

IMPORTANT: This tool needs to be run before upgrading to GMS 2014 R2.

The tool is provided with the download of the GMS 2014 R2 iso. Follow the steps below to run the tool:

1. Download the GMSsslCheck.tar file to your GMS server.
2. Open a terminal and extract the contents of the tar file to a temporary location on your GMS server using the following command:

   ```
   tar xvf GMSsslCheck.tar
   ```

3. Open a terminal and browse to the folder where you extracted the files.
4. Run the following command:

   ```
   python sslcheck.pyc
   ```

5. In the menu prompt, select option `1`.

   The tool connects to all of your GroupWise POAs and checks their SSL settings against the GMS settings. If the settings do not match those in GMS, the information is displayed so you can resolve the settings. Once the settings have been resolved, continue with the upgrade of GMS.

NOTE: If you are not upgrading but installing a new system, run MCheck after the installation and select the **System** > **SSL Check** option to check the SSL settings of your GroupWise POAs.

Certificate Verification

GroupWise Mobility Service 2014 R2 allows verification of the POA TLS/SSL certificate. After the installation or upgrade, certificate verification is disabled by default.

- Prerequisites
- Gathering CA Certificates
- Verifying the CA Certificates
- Adding the CA Certificates

- Enabling Certificate Verification
- Troubleshooting Certificate Verification

Prerequisites

- In the GroupWise Admin Console, the POA TCP/IP address needs to have the DNS name specified.
- In the Mobility Admin Console, the POA SOAP address needs to have the DNS name specified instead of the IP address.

Gathering CA Certificates

Follow the section that matches how you generated your POA certificates for each CA that you need to gather:

- GroupWise 2014 Certificate Authority
- NetIQ Certificate Server
- Trusted Commercial Certificate Authority

GroupWise 2014 Certificate Authority

If your CA is GroupWise (2014 or later), you can do one of the two methods below to get the certificate.

Method 1

1. Open a browser to `https://primarydomainip:adminport/gwadmin-service/system/ca`.

   For example: `https://10.10.10.10:9710/gwadmin-service/system/ca`
2. Enter your GroupWise admin credentials.
3. Save the certificate to the GMS server in `/var/lib/datasync/mobility`.
4. Continue with Verifying the CA Certificates if you have gathered all of your CA certificates.

Method 2

1. Open a terminal on your GMS linux server.
2. Enter the following command:

   `curl -k --user username -o filename https://primarydomainip:adminport/gwadmin-service/system/ca`

   Replace `username` with your admin username and `filename` with the name of the saved file.
3. Copy the certificate and then save it to the GMS server in `/var/lib/datasync/mobility`.
4. Continue with Verifying the CA Certificates if you have gathered all of your CA certificates.

NetIQ Certificate Server

If your CA is a NetIQ Certificate Server, follow the steps below:

1. Login to iManager.
2. Select **NetIQ Certificate Server**.

   It may be called **Novell Certificate Server** depending on your version of iManager.
3. Select **Configure Certificate Authority**.
4. Select the **Certificates** tab.
5. Select the **Self Signed Certificate** check box.
6. Select **Export**.
7. Unselect **Export private key**.
8. Select export formate as Base64.
9. Select **Next**.
10. Select **Save the exported certificate file**. Save it to the GMS server in `/var/lib/datasync/mobility`.
11. Continue with Verifying the CA Certificates if you have gathered all of your CA certificates.

Trusted Commercial Certificate Authority

If your CA is a commercial CA, follow the steps below:

1. Verify if your certificate is in the Mozilla trusted root CA store by checking the `/var/lib/datasync/mobility/cacert.pem` file on the GMS server where the CA store is stored. If your CA is in the list, continue with Verifying the CA Certificates if you have gathered all of your CA certificates.

   or
2. If your CA is no in the list, you need to find your CA public root certificate and place it on the GMS server in `/var/lib/datasync/mobility`. Continue with Verifying the CA Certificates if you have gathered all of your CA certificates.

Verifying the CA Certificates

Once you have your CA certificate, make sure it meets the following requirements:

- Base64-encoded format
- In the `Basic Constraints`, ensure that `Subject Type=CA` is specified.
- Ensure that the current date is between the `Valid from` and `Valid to` dates.
- The `Issuer` and the `Subject` match.

You can verify these requirements by viewing the details of the certificate or by running an openssl command to view the certificate information.

If your CA meets these requirements, continue with Adding the CA Certificates.

Adding the CA Certificates

For the certificate verification to work, the CA certificates found previously needs to be added to the mob_ca.pem file. Follow the section that matches each CA certificate you gathered previously:

- "GroupWise 2014 Certificate Authority" on page 3
- "NetIQ Certificate Server" on page 3
- "Commercial Certificate Authority" on page 3

GroupWise 2014 Certificate Authority

1. In a terminal on your GMS server, go to `/var/lib/datasync/mobility/`.
2. Add your CA certificate to the `mob_ca.pem` file using the following command:

   `cat yourCACertficate.pem >> mob_ca.pem`

   NOTE: You may need to add a hard return in the `mob_ca.pem` after the certificate before you add any other certificates to the file.
3. Continue with Enabling Certificate Verification if you have added all of your CA certificates.

NetIQ Certificate Server

1. In a terminal on your GMS server, go to `/var/lib/datasync/mobility/`.
2. Add your CA certificate to the `mob_ca.pem` file using the following command:

   `cat yourCACertficate.pem >> mob_ca.pem`

   NOTE: You may need to add a hard return in the `mob_ca.pem` after the certificate before you add any other certificates to the file.
3. Continue with Enabling Certificate Verification if you have added all of your CA certificates.

Commercial Certificate Authority

1. In a terminal on your GMS server, go to `/var/lib/datasync/mobility/`.
2. If your CA is not in the Mozilla CA certificate list, add your CA public certificate to the `mob_ca.pem` file using the following command:

   `cat yourCACertificate.pem >> mob_ca.pem`

   or

   If your CA is in the list, copy the cacert.pem file to `mob_ca.pem` using the following command:

   `cat cacert.pem >> mob_ca.pem`

   NOTE: You may need to add a hard return in the `mob_ca.pem` after the certificate before you add any other certificates to the file.
3. Continue with Enabling Certificate Verification if you have added all of your CA certificates.

Enabling Certificate Verification

Before you enable certificate verification, take a backup of the `/var/lib/datasync/mobility/mob_ca.pem` file.

1. Login to the GMS WebAdmin
2. Select **Config** > **GroupWise**.
3. Select **SSL Certification Verification**.
4. Select **Apply**.
5. In a terminal on the GMS server, restart GMS using the following command:

   `rcgms restart`

Troubleshooting Certificate Verification

You may experience SSL problems the first time you enable certificate verification. The following are helpful OpenSSL commands:

- Verify POA Connection
- Verify a Certificate
- View Certificate Information
- Get POA Certificate
- View Certificate Purpose

Verify POA Connection

`openssl s_client -showcerts -CAfile CA_public_certificate -connect poa_DNS:soap_port`

Example: `openssl s_client -showcerts -CAfile gwcacert.pem -connect gw.provo.novell.com:7191`

Verify a Certificate

`openssl verify -issuer_checks -CAfile CA_public_certificate POA_certificate`

Example: `openssl verify -issuer_checks -CAfile cacert.pem gwpoa.pem`

View Certificate Information

`openssl x509 -in certificate -noout -text`

Example: `openssl x509 -in gwcacert.pem -noout -text`

Get POA Certificate

`openssl s_client -showcerts -connect poa_DNS:soap_port`

Example: `openssl s_client -showcerts -connect gw.provo.novell.com:7191`

View Certificate Purpose

`openssl x509 -in` *`certificate`* `-noout -purpose`

Example: `openssl x509 -in gwcacert.pem -noout -purpose`