SHA1 Certificate Upgrade Plan

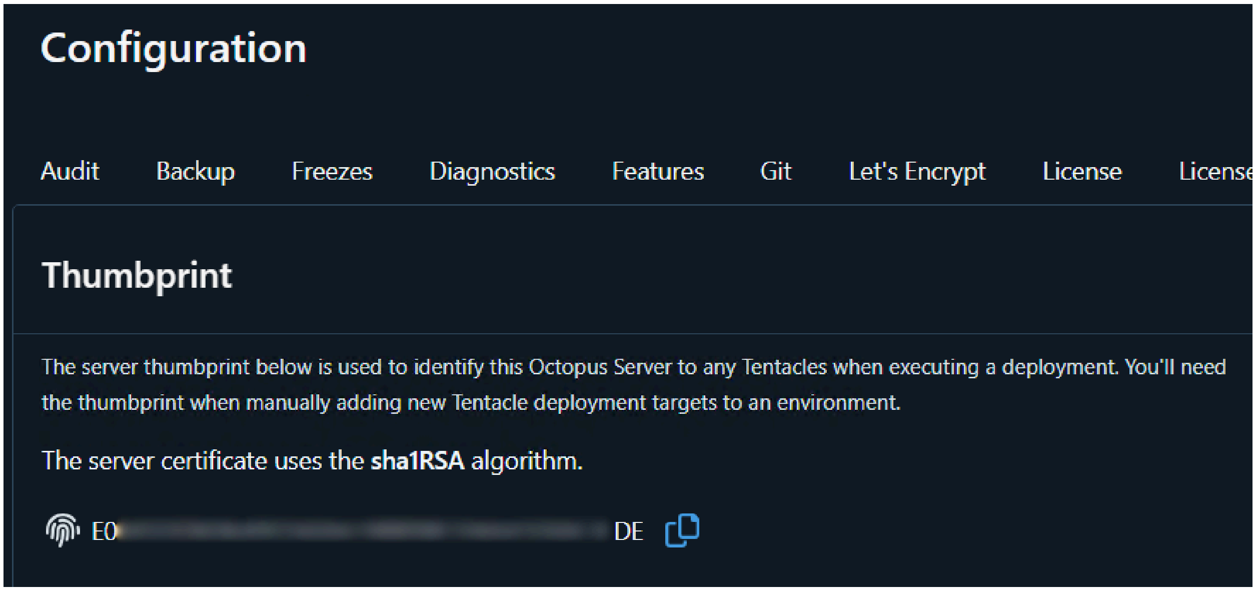
*NB: This plan needs to be run **only** if your self-hosted Octopus Server is still using a SHA1 thumbprint / certificate.*

This process is not necessary for Octopus Cloud unless you are migrating from an older self-hosted Octopus Server instance to Octopus Cloud; in which case we recommend you speak to our Support Team, support@octopus.com first.

Introduction

Most of the scripts referenced here, come from this web page, *and are suitable for self-hosted Octopus Server instances that run on a single server **or** Octopus Server HA clusters.*

Q: How do you know if your self-hosted Octopus Server is still using a SHA1 certificate/thumbprint?
A: Go to **Configuration** > **Thumbprint** and look for either **sha1RSA** or **sha256RSA** on that screen.



The server thumbprint below is used to identify this Octopus Server to any Tentacles when executing a deployment. You'll need the thumbprint when manually adding new Tentacle deployment targets to an environment.

The server certificate uses the **sha1RSA** algorithm.

E0[redacted]DE

If you see ***sha1RSA***, then you should proceed with the plan below:

Q: Besides my Octopus Server instance, how do I know which of my *targets* are using SHA1 certificates?
A: To check, either curl the API, or use the PowerShell script found here.

For both curl and the PS script you'll need an *Octopus API key* and your *Octopus Server's hostname* as well as the *Space ID* you want to scan i.e. you'll need to run that script (or curl) multiple times if you have multiple spaces.

Here's an example curl command if you can't use PowerShell:

```
'curl -H "X-Octopus-Apikey: API-XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX" -H
"Accept: application/json"
"https://<instance-hostname>/api/<space-id>/machines" |  jq '.Items
.[] | select(.Endpoint.CertificateSignatureAlgorithm=="sha1RSA")'
```

The above curl command can also be found in `0WhichTentaclesHaveSHA1Certs.bat` in the accompanying .zip file.

The Plan

This plan uses the .bat and .sh files found in the accompanying .zip file.

Also, please read through these instructions in their entirety before proceeding, and update the relevant user-specific fields and parameters in the scripts first before running them.

Pre-preparation

Octopus Server

Step 1: From an elevated prompt on one Octopus Server HA node, run the `1OctopusServer-BackupOctopusServerCertAndThumbprint.bat` script to backup the existing SHA1 cert (sometimes referred to as 'the Halibut certificate').

a. Again from an elevated prompt, now generate a new SHA256 cert using the `2OctopusServer-CreateNewOctopusServerCertAndThumbprint.bat` script.

Note: You have only created a new (SHA256) certificate, **it is not yet active** in Octopus Server.

Listening & Polling Tentacle / targets

Note: Listening targets are able to trust more than one cert / thumbprint, so there will be no downtime. Polling tentacles cannot do this. This means there will be downtime for Polling targets until you have completed this process i.e. leave Polling Tentacles until Action Day.

Listening Tentacles

Step 2: Copy the new cert .pfx over to all the targets that need it (you could copy the outputted .pfx to a common file share accessible across your network and reference it from there - if your network topology and company security policies allows that), and then from an elevated prompt, run the Tentacle trust `3WindowsTentacle-TrustNewCert.bat` or `3LinuxTentacle-TrustNewCert.sh` script - depending on your operating system.

You do not need to restart the Tentacle service as there is already a command in those scripts that will do this for you.

Note: As Listening Tentacles can have more than one thumbprint that they trust, Step 2 is fine to run on all listening targets regardless of the environment they are in i.e. *Step 2 is Production-safe for Listening Tentacles*.

Polling Tentacles

Due to the fact that Polling Tentacles are only able to trust one Octopus Server certificate / thumbprint at a time, there will be downtime while the cert is updated on all targets where a Polling Tentacle has been installed.

Action Day

Octopus Server

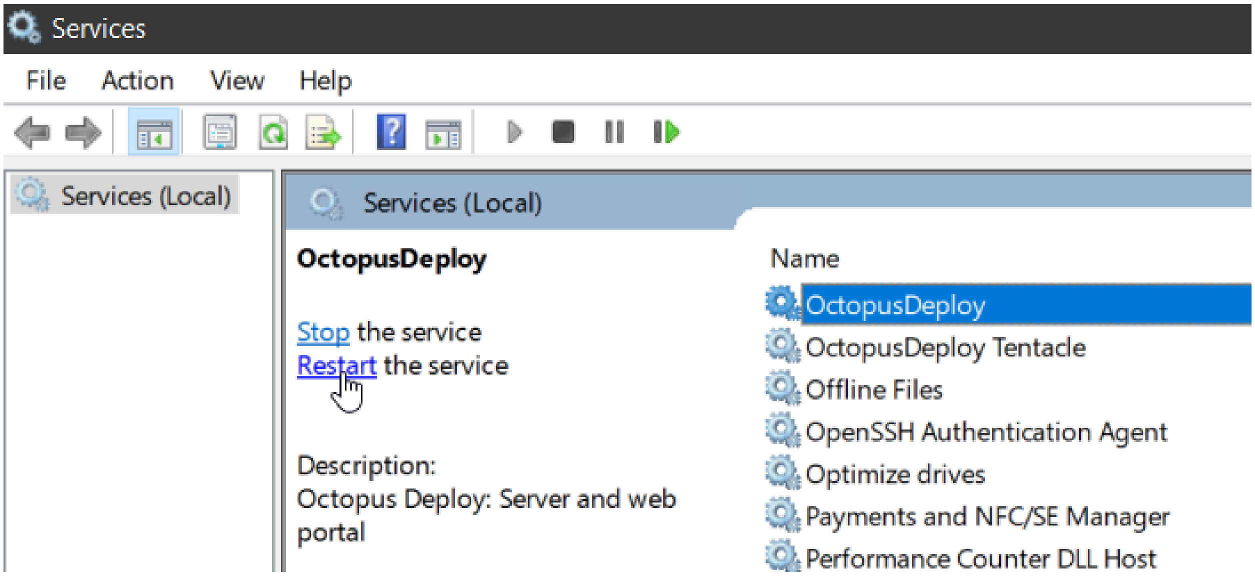
Step 1. On the day you decide to start using the new SHA256, then:

a. On one HA node, import the new SHA256 into Octopus Server by running the `4OctopusServer-ImportNewCertIntoEachHANode.bat` script in an elevated prompt.

This is the command that will replace the existing SHA1 cert.

You do not need to restart the OctopusDeploy service on the node where you ran the command as there is already a command in that script that will do this for you.

b. If you have an HA cluster then you *must* restart the **OctopusDeploy** service on each of the *other* HA nodes.



OctopusDeploy

Stop the service
Restart the service

Description:
Octopus Deploy: Server and web portal

- OctopusDeploy
- OctopusDeploy Tentacle
- Offline Files
- OpenSSH Authentication Agent
- Optimize drives
- Payments and NFC/SE Manager
- Performance Counter DLL Host

Note: A reboot of the server(s) is **not** required.

Polling Tentacles

On the same day that you start using the new SHA256 certificate:

Step 2: Copy the new cert .pfx over to all the targets that need it (you could copy the outputted .pfx to a common file share and reference it from there - if your network topology and company security policies allows that), and then from an elevated prompt, run the Tentacle trust `5Polling-WindowsTentacle-TrustNewCert.bat` or `5Polling-LinuxTentacle-TrustNewCert.sh` script - depending on your operating system.

You do not need to restart the Tentacle service as there is already a command in those scripts that will do this for you.

Listening Tentacles

Listening Tentacles already trust the new certificate / thumbprint, so go straight to the Clean up step below.

Clean up

Step 3. Again, from an elevated prompt on *each* Listening target, run the `5WindowsTentacle-StopTrustingOldOctopusServerCert.bat` or `5LinuxTentacle-StopTrustingOldOctopusServerCert.sh` script, to remove the old SHA1 certificate.

Note: You ***must not*** run the above clean up command on any Polling Tentacles!

Again, you do not need to restart the Tentacle service as there is already a command in those scripts that will do this for you.

Finally, do some test deployments to ensure communications are working as expected.

Help

If you have any questions prior to executing this plan, or you experience any issues or need help confirming what you need to do, please reach out to your TAM (if you have one), or email our Support Team at: support@octopus.com, thank you.