

VMware Cloud Director Availability On-premises Guides

Guide #17

Managing Certificates

You can find the most up-to-date technical documentation on the VMware website at: <https://docs.vmware.com/>

If you have comments about this documentation, submit your feedback to: vcav-light@vmware.com

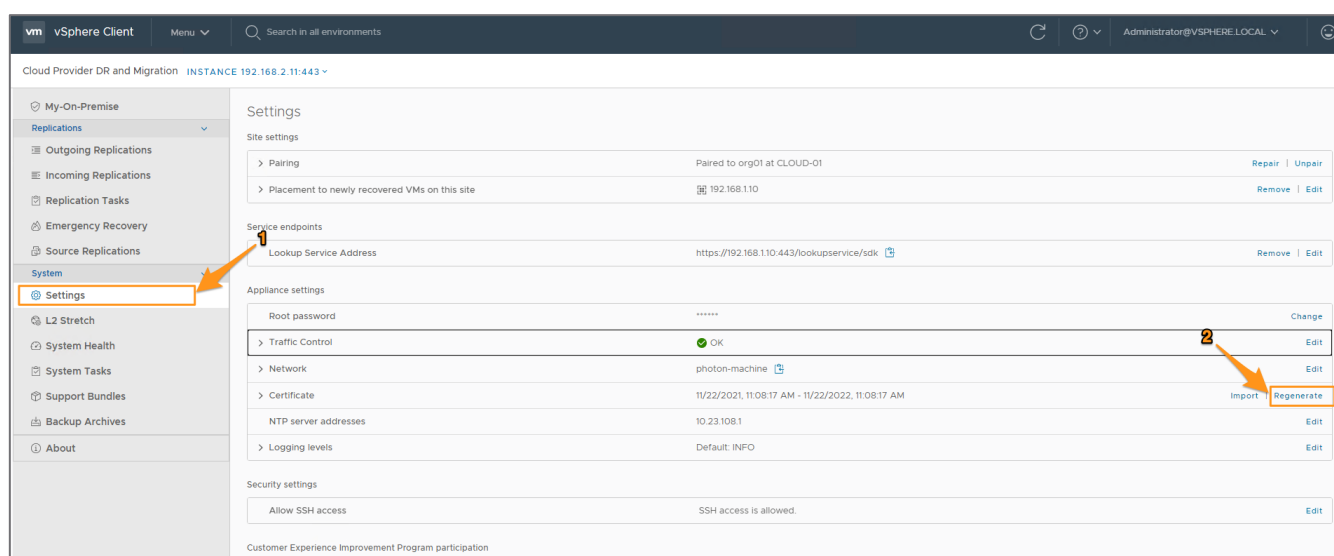
If the replicator certificate is about to expire or to replace a self-signed certificate with a signed certificate, the self-signed certificate can be regenerated or a signed certificate can be imported.

Note: For operation without service interruptions, it is important that before the expiration date of the current certificate, the self-signed certificate must be regenerated or the new signed certificate must be imported.

Self-signed certificate regeneration

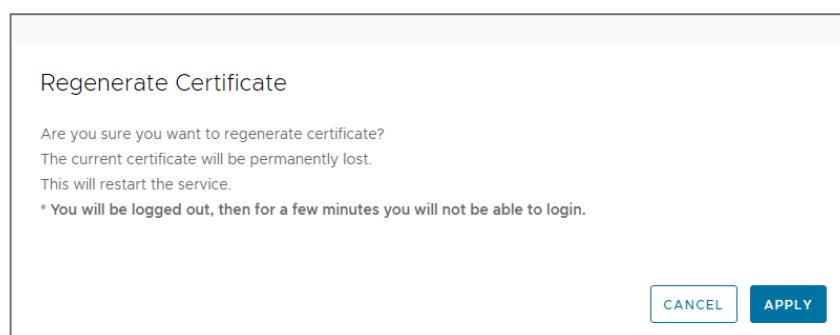
To regenerate the self-signed certificate of the replicator:

1. In the left pane, click **Settings**.
2. Under Appliance settings, next to Certificate click the Regenerate link.

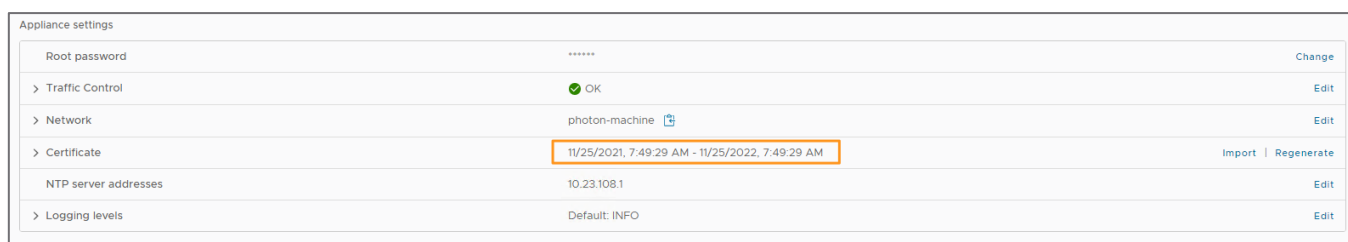


3. In the **Regenerate Certificate** window click **Apply**.

Note: The replicator restarts and after a few minutes resumes operations.



4. Log back in and under **Appliance settings**, next to **Certificate** validate the new certificate expiration date.

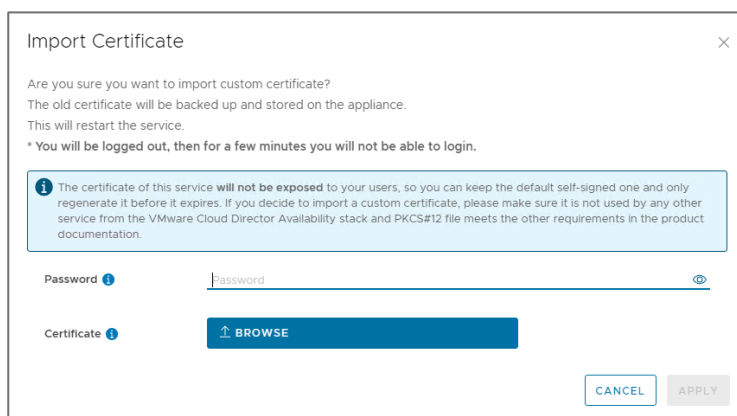


Import signed certificate

To import a signed certificate for the replicator:

1. In the left pane, click **Settings**.
2. Under Appliance settings, next to Certificate click the Import link.
3. In the **Import Certificate** window, to upload a certificate click **Browse**, provide the certificate password and click **Apply**.

Note: The replicator restarts and after a few minutes resumes operations.



Import Certificate

Are you sure you want to import custom certificate?
The old certificate will be backed up and stored on the appliance.
This will restart the service.
* You will be logged out, then for a few minutes you will not be able to login.

i The certificate of this service **will not be exposed** to your users, so you can keep the default self-signed one and only regenerate it before it expires. If you decide to import a custom certificate, please make sure it is not used by any other service from the VMware Cloud Director Availability stack and PKCS#12 file meets the other requirements in the product documentation.

Password **i**

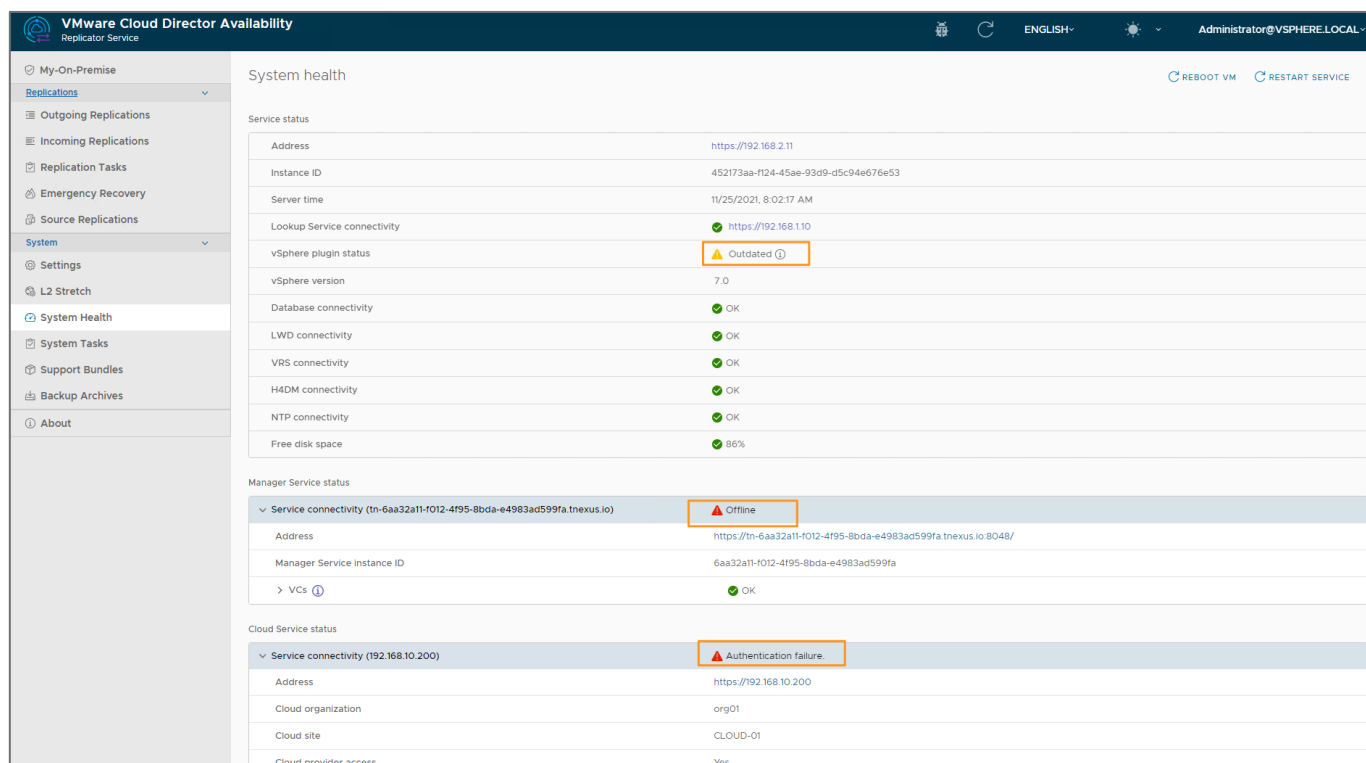
Certificate **i** **BROWSE**

CANCEL **APPLY**

4. Log back in and under **Appliance settings**, validate the signed certificate by expanding the Certificate section.

Update the Lookup Service registration and repair the cloud site

After importing a new certificate or regenerating the self-signed certificate, the Lookup Service registration and the cloud pair must be updated.



VMware Cloud Director Availability
Replicator Service

System health

Service status

Address	https://192.168.2.11
Instance ID	452173aa-f124-45ae-93d9-d5c94e676e53
Server time	11/25/2021, 8:02:17 AM
Lookup Service connectivity	https://192.168.1.10
vSphere plugin status	Outdated i
vSphere version	7.0
Database connectivity	OK
LWD connectivity	OK
VRS connectivity	OK
H4DM connectivity	OK
NTP connectivity	OK
Free disk space	86%

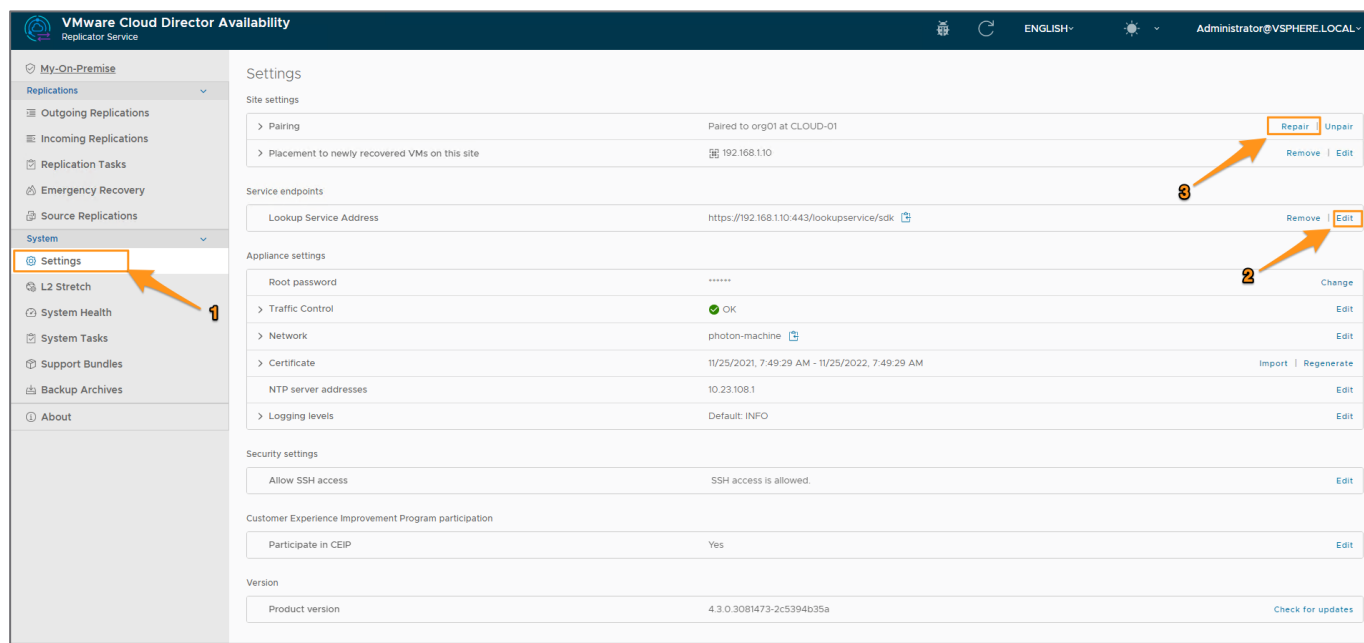
Manager Service status

Service connectivity (tn-6aa32a11-f012-4f95-8bda-e4983ad599fa.tnexus.io)	Offline
Address	https://tn-6aa32a11-f012-4f95-8bda-e4983ad599fa.tnexus.io:8048/
Manager Service instance ID	6aa32a11-f012-4f95-8bda-e4983ad599fa
> VCs i	OK

Cloud Service status

Service connectivity (192.168.10.200)	Authentication failure
Address	https://192.168.10.200
Cloud organization	org01
Cloud site	CLOUD-01
Cloud provider access	Yes

1. In the left pane, click **Settings**.
2. To update the Lookup Service registration, under **Service endpoints** next to **Lookup Service Address** click the **Edit** link (2) and provide the Lookup Service SSO credentials.
3. To update the cloud site pairing, under **Site details**, next to **Pairing** click the **Repair** link (3) and follow the wizard as per the **Pair steps in Guide # 7. Connect to the provider cloud.**



4. **Optional:** Verify **Incoming Replications** and **Outgoing Replications** status to validate that the replications are operational after the certificate replacement.



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Copyright © 2020 VMware, Inc.
All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions.
All other marks and names mentioned herein may be trademarks of their respective companies. Item No: vmw-wp-tech-temp-a4-word-101-proof 6/20