CredHub Service Broker

CredHub Service Broker services

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

https://techdocs.broadcom.com/

Contents

Overview of CredHub Service Broker

CredHub Service Broker allows apps running on VMware Tanzu Application Service for VMs (TAS for VMs) to access secure credentials in CredHub.

Apps can use these credentials to authenticate with services not on TAS for VMs, including services running on Tanzu Operations Manager such as Spring Cloud Services and services external to Tanzu Operations Manager.

The CredHub Service Broker uses secure binding credentials to prevent credential exposure in the app environment.

Overview

The CredHub Service Broker registers a service broker with TAS for VMs and exposes its service plans on the Marketplace. Developers can then create service instances using Apps Manager or the Cloud Foundry Command Line Interface (cf CLI) and bind them to their apps.

Creating a CredHub Service Broker instance and binding it to an app creates a credential in CredHub and provides the reference to that credential in the app environment. This allows developers to deploy apps that can securely access credentials for services that are not running on TAS for VMs.

Key Feature

The key feature of CredHub Service Broker is secure access to service credentials for services that are not running on TAS for VMs.

Product Snapshot

The following table provides version and version-support information about the v1.6 release line of CredHub Service Broker.

Element	Details
Tile version	v1.6.4
Release date	July 29, 2024
Software component version	v1.6.4
Compatible Tanzu Operations Manager versions	3.0
Compatible TAS for VMs versions	4, 5, and 6
IaaS support	AWS, Azure, GCP, OpenStack, and vSphere
IPsec support?	Yes

The following table provides version and version-support information about the v1.5 release line of CredHub Service Broker.

Element	Details
Tile version	v1.5.5
Release date	February 20, 2024
Software component version	v1.5.5
Compatible Tanzu Operations Manager versions	2.10, 3.0
Compatible TAS for VMs versions	2.11, 2.13, 3, and 4
IaaS support	AWS, Azure, GCP, OpenStack, and vSphere
IPsec support?	Yes

Requirements

CredHub Service Broker has the following requirement:

- Secure binding credentials enabled in runtime CredHub

To enable secure binding credentials in runtime CredHub, see Securing Services Instance Credentials with Runtime CredHub.

Installing and Configuring CredHub Service Broker

This topic tells you how to install and configure CredHub Service Broker.

Prerequisites

To install and configure the CredHub Service Broker, you must have CredHub instances available in your VMware Tanzu Application Service for VMs (TAS for VMs) deployment.

To confirm the number of CredHub instances available, perform the following actions:

1. Click the **TAS for VMs** tile in the Tanzu Operations Manager Installation Dashboard.

2. Select the **Resource Config** tab.

3. Locate the **CredHub** job and verify that the number of instances is set to at least 1.

   The number of instances that you need depends on both the version of TAS for VMs and whether or not you want high availability:

In TAS for VMs version…	For high availability, set to…	Default value is…
2.7 and earlier	2 or more	0
2.8 and later	3 or more	2

For more information on installing and configuring TAS for VMs for your chosen IaaS, see TAS for VMs.

Install CredHub Service Broker

To install the CredHub Service Broker tile on the Tanzu Operations Manager Installation Dashboard, do the following:

1. Download the product file from Broadcom Support Portal.

2. Go to the Tanzu Operations Manager Installation Dashboard and click **Import a Product** to upload the product file.

3. Under the **Import a Product** button, click **+** next to the version number of CredHub Service Broker. This adds the tile to your staging area.

Configure CredHub Service Broker

To configure the CredHub Service Broker:

1. Click the newly added **CredHub Service Broker** tile.
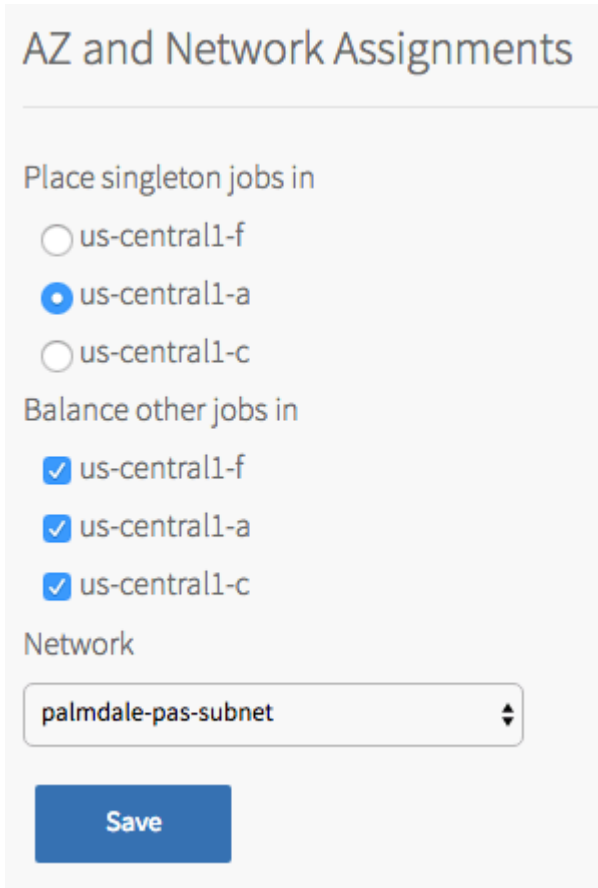
2. Follow the procedures below.

Configure AZs and Networks

To set the availability zones and network to deploy on, do the following:

1. Click **Assign AZs and Networks**.

2. Select a region under **Place singleton jobs in** and **Balance other jobs in**.

3. Select the **Network** where to deploy CredHub Service Broker. You may select any network.

4. Click **Save**

Configure Services Access

To confirm the default network that the CredHub Service Broker will be deployed on, do the following:

1. Click **Services Access**.

2. Ensure the **Enable global access to plans of service CredHub Service Broker** checkbox is selected.

3. Click **Save**

Configure Errands

To determine the errands will run after deployment and to ensure that the pre-delete errands will run if the tile is ever uninstalled, do the following:

1. Click **Errands**.

2. Ensure **deploy-all** is set to **Default (On)** under **Post-Deploy Errands**.

3. Ensure **delete-all** is set to **Default (On)** under **Pre-Delete Errands**.

4. Click **Save**.

Deploy CredHub Service Broker

To complete the installation and deploy the CredHub Service Broker tile, do the following:

1. Return to the Tanzu Operations Manager Installation Dashboard.

2. Click **Apply Changes** to deploy CredHub Service Broker.

Using CredHub Service Broker

This topic tells you how to use CredHub Service Broker.

Create and Bind a Service Instance

Creating a CredHub Service Broker instance and binding it to an app creates a credential in CredHub and provides the reference to that credential in the app environment. This allows you to deploy apps that can securely access credentials for services that are not running on VMware Tanzu Application Service for VMs (TAS for VMs).

To create a service instance of the CredHub Service Broker and bind it to your app:

1. Create a CredHub Service Broker service instance by running:

    ```
    cf create-service credhub default SERVICE-INSTANCE \
    -c '{"CREDENTIAL-NAME":"CREDENTIAL-VALUE"}'
    ```

    Where:

    - `SERVICE-INSTANCE` is a name for your new service instance.

    - `CREDENTIAL-NAME` is the name for the credential you want to provide to services that are not running on TAS for VMs.

    - `CREDENTIAL-VALUE` is the value of the credential.

    > ✎ You can provide multiple credentials as a JSON list. This JSON list has a maximum size of 64 KB. For example, `{"MY_CREDHUB_CRED": "1234", "MY_CREDHUB_CRED2": "5678"}`.

    For example:

    ```
    $ cf create-service credhub default my-credhub-instance \
    -c '{"MY_CREDHUB_CRED":"1234","MY_CREDHUB_CRED2":"5678"}'
    ```

2. Ensure that your app is written to use the credential that was provided through the service creation. `VCAP_SERVICES` is an environment variable that exists in every container.

    Access the `credhub` JSON object within `VCAP_SERVICES` to discover the credentials. For example, in Ruby you access this JSON object with `ENV['VCAP_SERVICES']['credhub']`.

    If you need to edit your app code, you must re-push the app before continuing.

3. Bind the CredHub Service Broker service instance to your app by running:

```
cf bind-service APP-NAME SERVICE-INSTANCE
```

4. Restart your app by running:

```
cf restart APP-NAME
```

5. Your app now has access to the credential created earlier. Verify that your credential is in the app environment by running the following command and locate the CredHub reference under VCAP_SERVICES in the output:

```
cf env APP-NAME
```

For example:

```
$ cf env my-app
Getting env variables for app my-app in org example / space example as
admin...
OK
System-Provided:
{
 "VCAP_SERVICES": {
  "credhub": [
   {
    "binding_name": null,
    "credentials": {
     "credhub-ref": "/credhub-service-broker/credhub/ac517e09-2f5e-475a
-bf87-ca4275faa536/credentials"
    },
    "instance_name": "credhub",
    "label": "credhub",
    "name": "credhub",
    "plan": "default",
    "provider": null,
    "syslog_drain_url": null,
    "tags": [
     "credhub"
    ],
    "volume_mounts": []
   }
  ]
 }
}
```

Update Credentials

To update credentials in an existing CredHub Service Broker service instance:

1. Run:

```
cf update-service SERVICE-INSTANCE \
```

```
-c '{"CREDENTIAL-NAME":"CREDENTIAL-VALUE"}'
```

Where:

- ○ `SERVICE-INSTANCE` is the name of your existing CredHub Service Broker service instance.

- ○ `CREDENTIAL-NAME` is the name for the updated credential you want to provide to services that are not running on TAS for VMs.

- ○ `CREDENTIAL-VALUE` is the value of the credential.

> ✎ You can update multiple credentials as a JSON list. For example,
> `{"MY_CREDHUB_CRED": "1234", "MY_CREDHUB_CRED2": "5678"}`.

For example:

```
$ cf update-service SERVICE-INSTANCE \
-c '{"MY_CREDHUB_CRED":"1234","MY_CREDHUB_CRED2":"5678"}'
```

2. Restart your app by running:

```
cf restart APP-NAME
```

Release Notes for CredHub Service Broker

This topic tells you about changes in different versions of CredHub Service Broker.

Long-Term Support for CredHub Service Broker

CredHub Service Broker v1.5 is the long-term supported (LTS) version of CredHub Service Broker. CredHub Service Broker v1.5 will be supported through February 2024.

Over the life cycle of each supported CredHub Service Broker version, VMware releases security patches that occasionally include bug fixes and maintenance updates.

v1.6.4

Release Date: July 29, 2024

Features

- Updated dependencies.

Known Issues

There are no known issues for this release.

v1.6.3

Release Date: February 20, 2024

Features

- Updated dependencies.

Known Issues

There are no known issues for this release.

v1.6.2

Release Date: November 3, 2023

Features

- Updated dependencies.

Known Issues

There are no known issues for this release.

v1.6.0

Release Date: September 28, 2023

Features

- Adds support for Jammy stemcell.
- Updated dependencies.

Known Issues

There are no known issues for this release.

v1.5.5

Release Date: February 20, 2024

Resolved Issues

- Updated dependencies

Known Issues

There are no known issues for this release.

v1.5.4

Release Date: November 3, 2023

Resolved Issues

- Updated dependencies

Known Issues

There are no known issues for this release.

v1.5.3

Release Date: October 13, 2023

Resolved Issues

- Updated dependencies

Known Issues

There are no known issues for this release.

v1.5.2

Release Date: June 1, 2023

Resolved Issues

- Updated dependencies.

Known Issues

There are no known issues for this release.

v1.5.1

Release Date: September 7, 2021

Resolved Issues

- The `unbind` request no longer fails if the service is already unbound.

Known Issues

There are no known issues for this release.

v1.5.0

Release Date: March 16, 2021

Resolved Issues

- The `deprovision` request no longer fails if the service is already deprovisioned.

Known Issues

There are no known issues for this release.

v1.4.8

Release Date: July 23, 2020

Resolved Issues

- Updated dependencies.

Known Issues

There are no known issues for this release.

v1.4.7

Release Date: December 13, 2019

Resolved Issues

- The `pre_start` script for `deploy-all` errands no longer fails on `python` calls.

Known Issues

There are no known issues for this release.

v1.4.6

Release Date: December 12, 2019

Resolved Issues

- The `pre_start` script for `deploy-all` is now compatible with Pivotal Application Service (PAS) v2.8.

Known Issues

This release has the following issue:

- The `pre_start` script for `deploy-all` errands fails on `python` calls.

v1.4.5

Release Date: November 1, 2019

Resolved Issues

- For PAS v2.7 and earlier, the `pre_start` script for `deploy-all` errands no longer fails on `awk` calls.

Known Issues

This release has the following issue:

- For PAS v2.8 and later, the `pre_start` script for the `deploy-all` errand fails on `jq` calls.

v1.4.4

Release Date: October 30, 2019

Resolved Issues

- Upgraded to Go v1.13.2 to patch a security vulnerability in Go's crypto/x509 library

Known Issue

This release has the following issue:

- The `pre_start` script for the `deploy-all` errand fails on `jq` calls. This is because `jq` does not exist on the stemcell.

v1.4.3

Release Date: October 4, 2019

Resolved Issues

- Upgraded to Go v1.13.1 to patch net/http vulnerability

Known Issues

There are no known issues for this release.

v1.4.2

Release Date: September 6, 2019

Resolved Issues

- Updated to Go v1.12.8 to patch HTTP/2 vulnerability

Known Issues

There are no known issues for this release.

v1.4.1

Release Date: August 7, 2019

Features

- Uses compiled releases in tile.

Known Issues

There are no known issues for this release.

v1.3.3

Release Date: July 2, 2019

Resolved Issues

- Fixes version number to return correctly without `rc`.

Known Issues

There are no known issues for this release.

v1.3.2

Release Date: June 13, 2019

Resolved Issues

- Updated CF_CLI dependency due to CVE

Known Issue

This release has the following issue:

- Version number contains `rc` despite it being a stable, public release. This is fixed in v1.3.3.

v1.3.1

Release Date: March 26, 2019

Features

- Adds support for Xenial stemcell

Known Issues

There are no known issues for this release.

v1.2.0

Release Date: November 26, 2018

Resolved Issues

- Updated Broker API dependency to v3.0.7 due to CVE 2018–15759
- Returns correct exit code when setting up the service broker

Known Issues

There are no known issues for this release.

v1.1.0

Release Date: November 9, 2018

Features

- Makes tile compatible with CredHub 2.0
- Makes tile compatible with Ops Manager 2.3 and Ops Manager 2.4

Known Issues

There are no known issues for this release.

v1.0.2

Release Date: June 6, 2018

Resolved Issues

- The tile now appropriately cleans up the deployed application service broker when uninstalled.

Known Issue

This release has the following issue:

- Upgrading the CredHub Service Broker tile from v1.0.0 and applying changes will fail.

  To upgrade to newer versions of the tile, uninstall CredHub Service Broker v1.0.0 and apply changes, and then add the newer version of the tile and apply changes again.

  Apps will lose access to credentials they are receiving through the CredHub Service Broker, and you must to re-create your services after reinstalling. All existing CredHub services are purged when uninstalling the CredHub Service Broker v1.0.0 tile.

v1.0.1

Release Date: May 7, 2018

Resolved Issues

- The tile now deploys alongside service brokers with nonrandom Plan IDs.

Known Issues

This release has the following issues:

- Removing the tile does not appropriately delete the service broker application. After uninstalling the tile or upgrading to a newer version, it is safe to delete the application manually.

- Upgrading the CredHub Service Broker tile from v1.0.0 and applying changes will fail.

  To upgrade to newer versions of the tile, uninstall CredHub Service Broker v1.0.0 and apply changes, and then add the newer version of the tile and apply changes again.

  Apps will lose access to credentials they are receiving through the CredHub Service Broker, and you must to re-create your services after reinstalling. All existing CredHub services are purged when uninstalling the CredHub Service Broker v1.0.0 tile.

v1.0.0

Release Date: April 12, 2018

First CredHub Service Broker for PCF release.

Features

- Provides secure access to service credentials for services that are not running on PAS

- Allows developers to pass custom JSON to their app through service creation

Known Issue

This release has the following issue:

- Upgrading the CredHub Service Broker tile from v1.0.0 and applying changes will fail.

  To upgrade to newer versions of the tile, uninstall CredHub Service Broker v1.0.0 and apply changes, and then add the newer version of the tile and apply changes again.

  Apps will lose access to credentials they are receiving through the CredHub Service Broker, and you must to re-create your services after reinstalling. All existing CredHub services are purged when uninstalling the CredHub Service Broker v1.0.0 tile.