Getting Started Guide **PUBLIC**

Document Version: 2.0 – 2022-06-02

How to create appliances with FQDN and Certificates in SAP Cloud Appliance Library

Table of Contents

Contents

Overview

SAP Cloud Appliance Library (https://cal.sap.com/) now provides the option to assign Fully Qualified Domain Names (FQDN) and signed certificates in the following cloud providers: *Amazon Web Services*, *Google Cloud Platform* and *Microsoft Azure*.

The appliances created from the appliance templates in SAP Cloud Appliance Library usually contain these settings, to allow fast and simple provisioning:

- A dummy domain name for Fiori access (*.dummy.nodomain)
- A certificate self-signed by SAP (issuer cal.dummy.nodomain)

With the help of defining FQDNs and creating certificates you can change these settings. As a result:

1. Users can easily access an appliance (or the application on it) from their computer right after the appliance creation without any additional configuration like changing local etc/hosts file.
2. Custom FQDN can be used to reach an appliance in SAP Cloud Appliance Library. This also simplifies the integration of the relevant application into your corporate infrastructure.
3. Self-signed certificates for the user access can be avoided, which might be denied from corporate proxies or web browsers.

Setting up this feature as described in the next paragraphs works for DNS enabled appliance templates in SAP Cloud Appliance Library.

Setup Prerequisites

Hypescaler Environment

The hyperscaler environment needs to be prepared with a dedicated domain, load balancers and certificates to make use of this feature in SAP Cloud Appliance Library.

There are a few general prerequisites that must be configured before using this feature. The following prerequisites apply for all hyperscalers:

- Have a well-defined valid hosted zone in the hyperscaler.
- Assign the cloud credentials of SAP Cloud Appliance Library the necessary permissions for the hyperscaler DNS service.
- Assign the cloud credentials of SAP Cloud Appliance Library the necessary permissions for the hyperscaler certificate service.

The detailed hyperscaler specific prerequisites (for example, regarding permissions) are given in the sections about Amazon Web Services (AWS), Google Cloud Platform (GCP), Microsoft Azure, and need to be configured before using the feature.

Note that there will be a **minimal increase of costs** for running the appliance. The cost forecast in the SAP Cloud Appliance Library will indicated this for the appliance.

Additional costs include:

- Load balancers (Network Load balancers in AWS, Application Gateways in Microsoft Azure, forwarding rules in GCP. These costs are included in the SAP Cloud Appliance Library cost forecast calculations:
  - AWS Load balancing cost details
  - Azure Application Gateway cost details
  - GCP forwarding rule cost details

  Load balancer traffic is not part of SAP Cloud Appliance Library cost forecast calculations as it cannot be presumed in advance

- DNS service costs. This is not part of SAP Cloud Appliance Library cost forecast calculations as it cannot be presumed in advance.
  - AWS Route 53
  - Microsoft Azure DNS
  - Google Cloud Provider

Once the infrastructure in the cloud provider is set up, you can use it for creating appliances but can also stick to the default appliance setup using the dummy domain.

If you want to switch back an appliance that was created with the FQDN feature to the default setup you need to apply some changes in the system itself (see configuration automation in the section below)

Appliance with FQDN and Certificates

After the configuration of your Hyperscaler environment an appliance from a DNS enabled appliance template can be created in SAP Cloud Appliance Library.

The appliance creation for S/4HANA Fully activated appliance templates and Solution Manager Demo appliance templates includes automation reflecting the infrastructure changes. HTTPURLLOC and the HTTP destinations in ABAP (se59) are adapted to reflect the FQDN.

For more information, see Creating an Appliance using your Domain and Certificates in SAP Cloud Appliance Library.

Certificate Lifecycle

Hyperscalers enable their customers to issue and or/import certificates that can be used with their services. SAP Cloud Appliance Library uses these features on behalf of SAP Cloud Appliance Library customers.

An important note on certificate lifecycle must be made on renewal:

- Manually imported certificates to the hyperscalers will not be automatically renewed.
- Automatically issued certificates by hyperscalers will be renewed automatically provided that hyperscalers conditions are followed.
    - In AWS that the validation DNS entries in Route53 are still resolvable.
    - In GCP that the certificate is still attached to a forwarding rule that is still available and that the forwarding rule IP is resolvable through its DNS records.

Note that in Microsoft Azure, SAP Cloud Appliance Library currently uses only imported certificates.

FQDN and Certificate Options in AWS

Do not use a domain name - rely on IP addresses only

This is the scenario that is supported in the default appliance creation process:

Virtual hostnames such as *cal.dummy.nodomain* are assigned and self-signed certificates are prepared. For easy appliance access users might need to change locale setting on their computer. For more information, see the Overview section in this document.

A typical URL to SAP Fiori Launchpad in such an appliance looks like this:

https://vhcals4hcs.dummy.nodomain:44301/sap/bc/ui5_ui5/ui2/ushell/shells/abap/FioriLaunchpad.html

Use a default domain name

These are domain names based on the AWS Appliance IP Addresses. In SAP Cloud Appliance Library, this option requires static IP addresses. For more information, see the AWS documentation.

Use dedicated domain name (needed for the FQDN feature)

This option uses a hosted zone registered in your cloud provider account. It enables the usage of certificates registered in your cloud provider account.

Moreover, this option enables customers to use already imported certificates or issue new certificates for your appliance using the AWS Certificate Manager Services.

Configure Permissions in AWS

You need to assign the following permissions in the AWS Management Console:

- Route 53 permissions to the IAM user.
  SAP Cloud Appliance Library requires permissions for listing, describing hosted zones as well as **ChangeResourceRecordSets**. For more information, see the AWS documentation.

- AWS ACM permissions to the IAM user.
  For more information, see the AWS documentation.

- AWS ELB permissions to the IAM user.
  For more information, see the AWS documentation.

SAP Cloud Appliance Library will create a load balancer with the certificate that will route the user requests to the respective virtual machine in your SAP Cloud Appliance Library appliance. You can choose this option during appliance creation.

FQDN and Certificate options in GCP

Do not use a domain name - rely on IP addresses only

This is the scenario that is supported in the default appliance creation process:

Virtual hostnames such as *cal.dummy.nodomain* are assigned and self-signed certificates are prepared. For easy appliance access users might need to change locale setting on their computer. For more information, see the Overview section in this document.

A typical URL to SAP Fiori Launchpad in such an appliance looks like this:

https://vhcals4hcs.dummy.nodomain:44301/sap/bc/ui5_ui5/ui2/ushell/shells/abap/FioriLaunchpad.html

Use a default domain name

This option is not available for Google Cloud Platform.

Use dedicated domain name (needed for the FQDN feature)

This option uses a hosted zone registered in your cloud provider account. It enables the usage of certificates registered in your cloud provider account. For more information, see the GCP documentation

Moreover, this option enables customers to use already imported certificates or issue new certificates for your appliance using the Google Managed Certificates.

Configure Permissions in GCP

You need to assign Cloud DNS permissions to the service account that is configured in SAP Cloud Appliance Library. For more information, see the GCP Documentation.

SAP Cloud Appliance Library will create a load balancer with the certificate that will route the user requests to the respective virtual machine in your SAP Cloud Appliance Library appliance. You can choose this option during appliance creation.

FQDN and Certificate options in Microsoft Azure

Do not use a domain name - rely on IP addresses only

This is the scenario that is supported in the default appliance creation process:

Virtual hostnames such as *cal.dummy.nodomain* are assigned and self-signed certificates are prepared. For easy appliance access users might need to change locale setting on their computer. For more information, see the Overview section in this document.

A typical URL to SAP Fiori Launchpad in such an appliance looks like this:

https://vhcals4hcs.dummy.nodomain:44301/sap/bc/ui5_ui5/ui2/ushell/shells/abap/FioriLaunchpad.html

Use a default domain name

These domain names start with a specified label and resolves to static public IP addresses. They will be registered with the Azure-provided DNS servers. In SAP Cloud Appliance Library, this option requires static IP addresses.

Use dedicated domain name (needed for the FQDN feature)

This option uses a hosted zone registered in your cloud provider account. It enables the usage of certificates registered in your cloud provider account.

Configure Permissions in Microsoft Azure

To use certificates, you need *Key Vault permissions*:

Azure Key Vault is a service that lets you easily provision, manage, and deploy public and private Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates for use with Azure and your internal connected resources. For more information about key vaults, see the official Azure documentation.

Certificates in Microsoft Azure can be issued by Microsoft Azure's partners. For more information, see official Azure Documentation

To use certificates registered in a key vault, you must grant access to SAP Cloud Appliance Library principal. To enable the usage of Azure certificates in the SAP Cloud Appliance Library system, you must execute the following steps:

1. Go to the Microsoft Azure Portal: https://portal.azure.com/.
2. From the main menu, go to *Key Vaults*.
3. Find and select the key vault you want to use.
4. Go to *Access Control*.
5. Choose *Add* and then choose *Add role assignment*.
6. For Role, select *Reader*.
7. Assign this role to *SAP Cloud Appliance Library Extended*.
8. Choose *Save*.
9. Go to *Access Policies* and choose *Add access policy*.
10. From the *Configure from template input*, choose *Secret and Certificate Management*.
11. Select a principal and choose *SAP Cloud Appliance Library Extended*.
12. Choose *Add* and then *Save*.

SAP Cloud Appliance Library will create an application gateway which is a web traffic load balancer. It will configure it with the selected certificate and route the end user requests to your virtual machines. For more information on Azure Application Gateways, see the MS Azure Documentation.

You can choose this option during appliance creation in SAP Cloud Appliance Library.

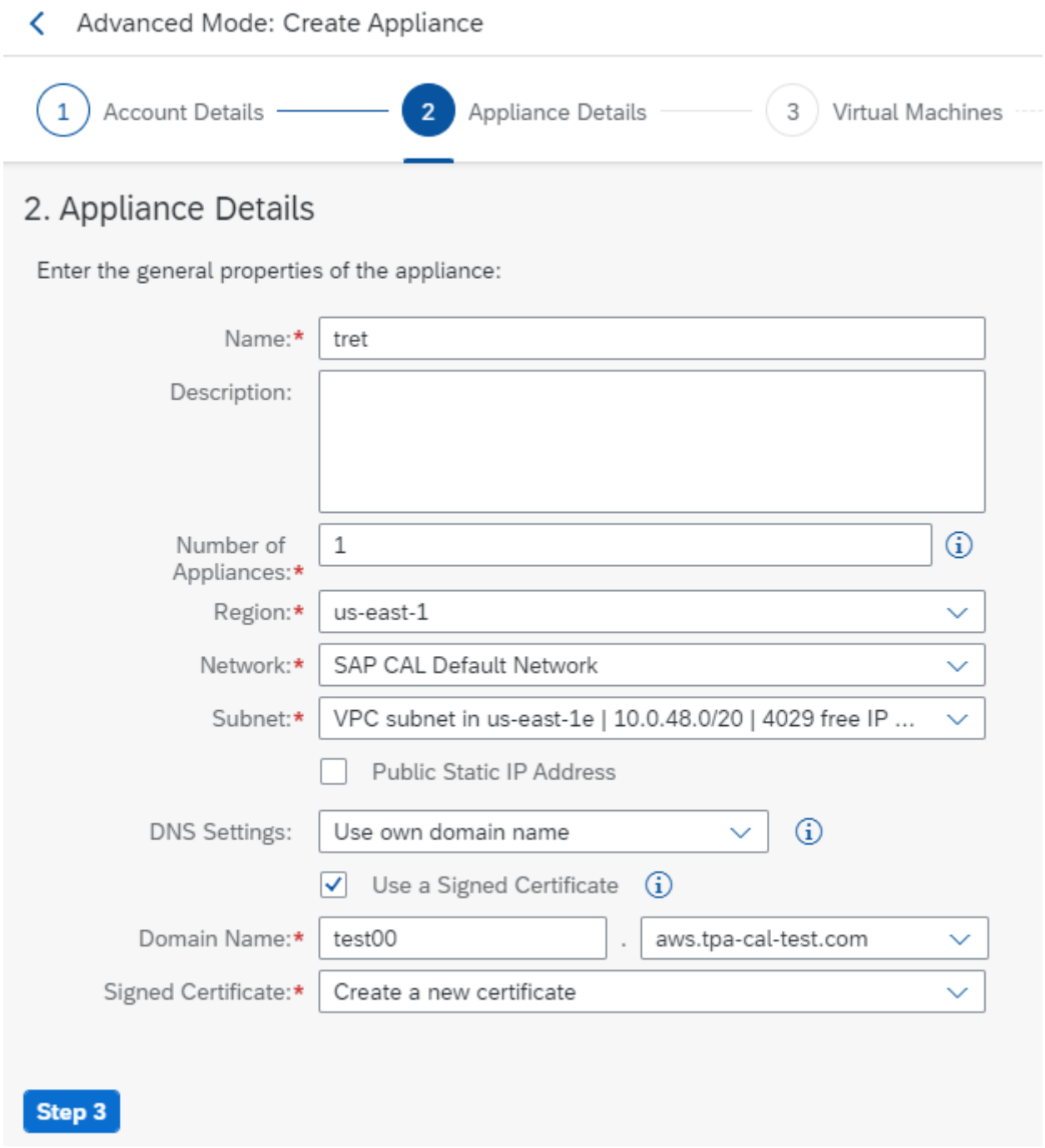
Creating an Appliance using your Domain and Certificates in SAP Cloud Appliance Library

You have two modes from which you can choose to create an appliance in SAP Cloud Appliance Library:

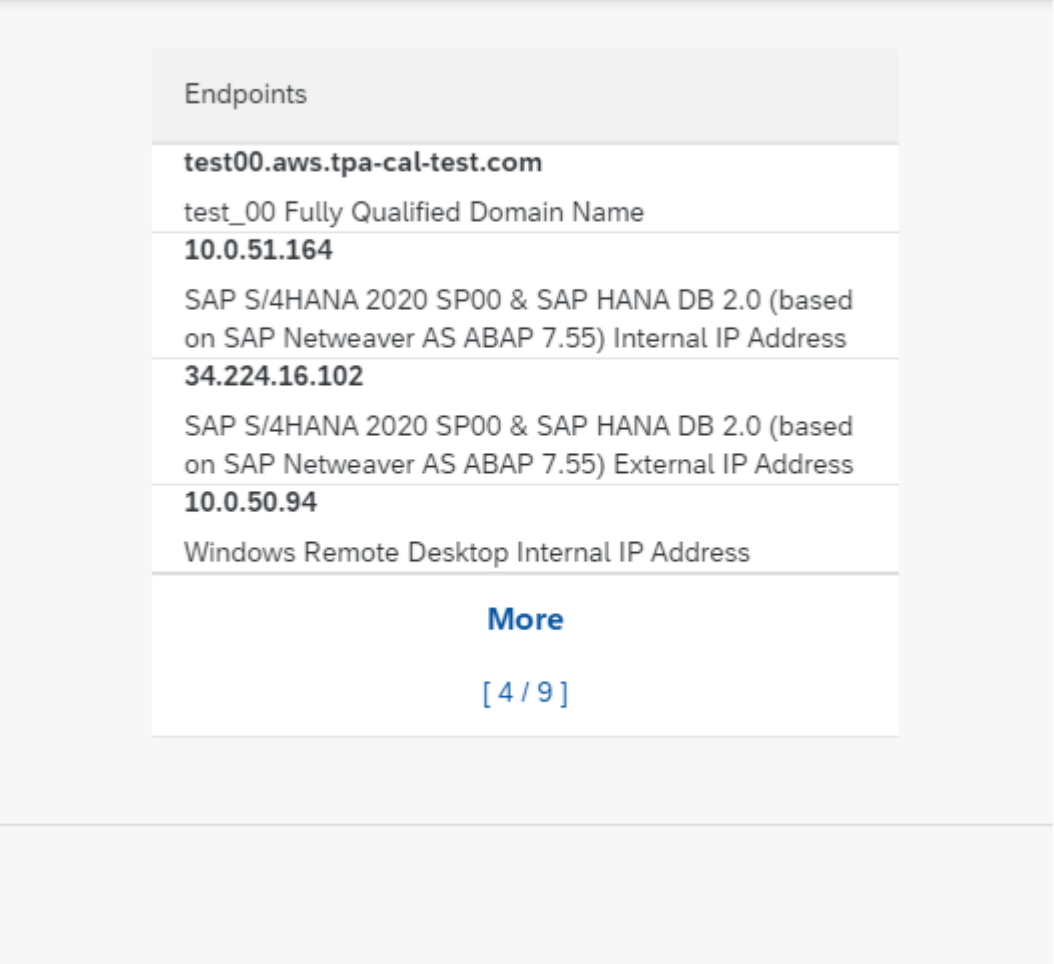
- **Basic Mode**: With this mode you can quickly create your appliance configuring only the basic details of the appliance. For more information, see Basic Mode: Creating an Appliance.
- **Advanced Mode**: With this mode you can create your appliance going through a wizard specifying all appliance configurations. For more information, see Advanced Mode: Creating an Appliance.

To use this feature (FQDN and Certificates) you must choose the *Advanced Mode* when you create appliance in SAP Cloud Appliance Library and go to the *Appliance Details* step from the *Create Appliance* wizard.

1. In the *Appliance Details* step, you will see *DNS Settings* dropdown list from where you can select your option depending on your scenario and the cloud provider. Choose own domain name.
2. Specify the *Domain Name* and the *Certificate* that you want to use for your scenario:



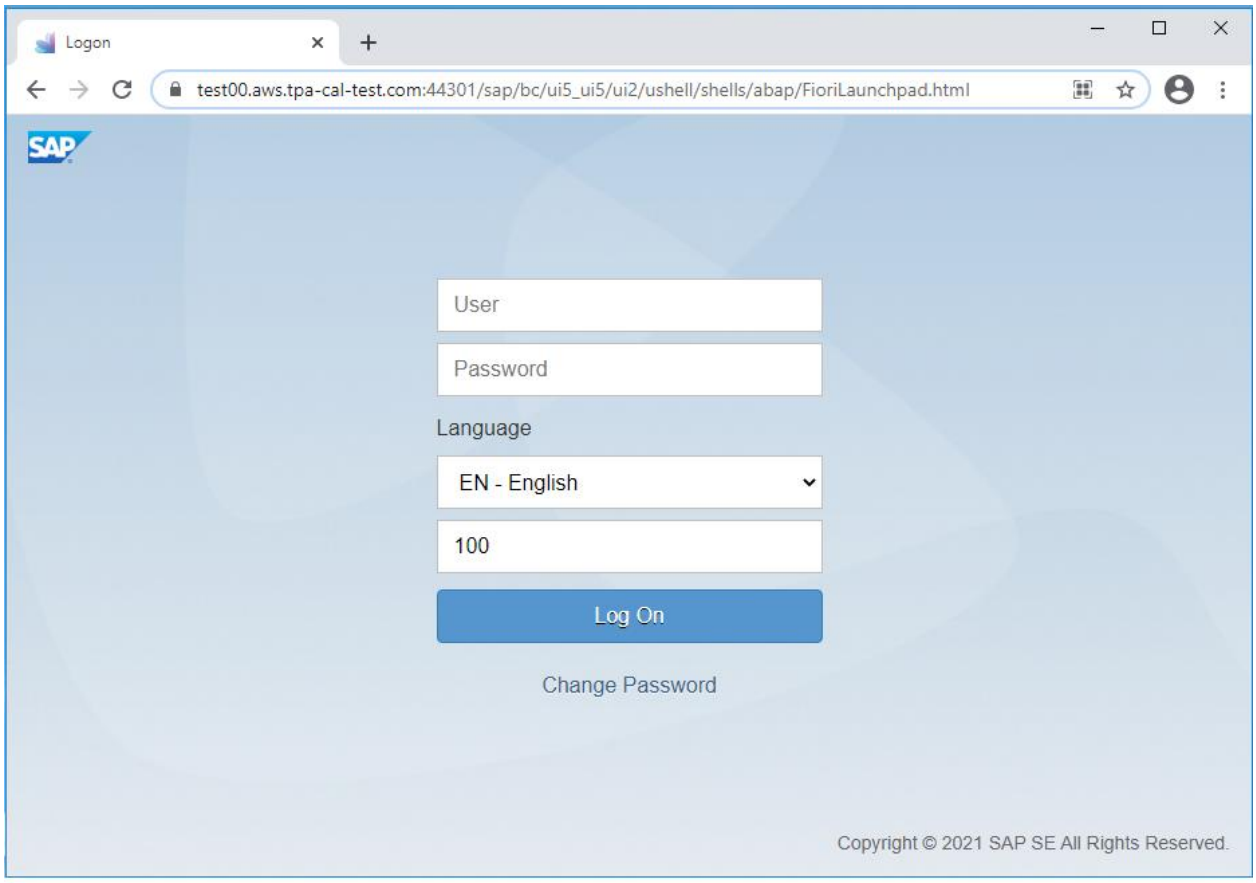
3. During appliance creation you will see that an additional end point is created, in the example here: **test00.aws.tpa-cal-test.com**



4. Once the appliance is active you can directly logon to e.g. SAP Fiori Launchpad without further configuration of local files or being prompted to accept self-signed certificates.

With the setting chosen in the example here the SAP Fiori Launchpad URL now looks like this:

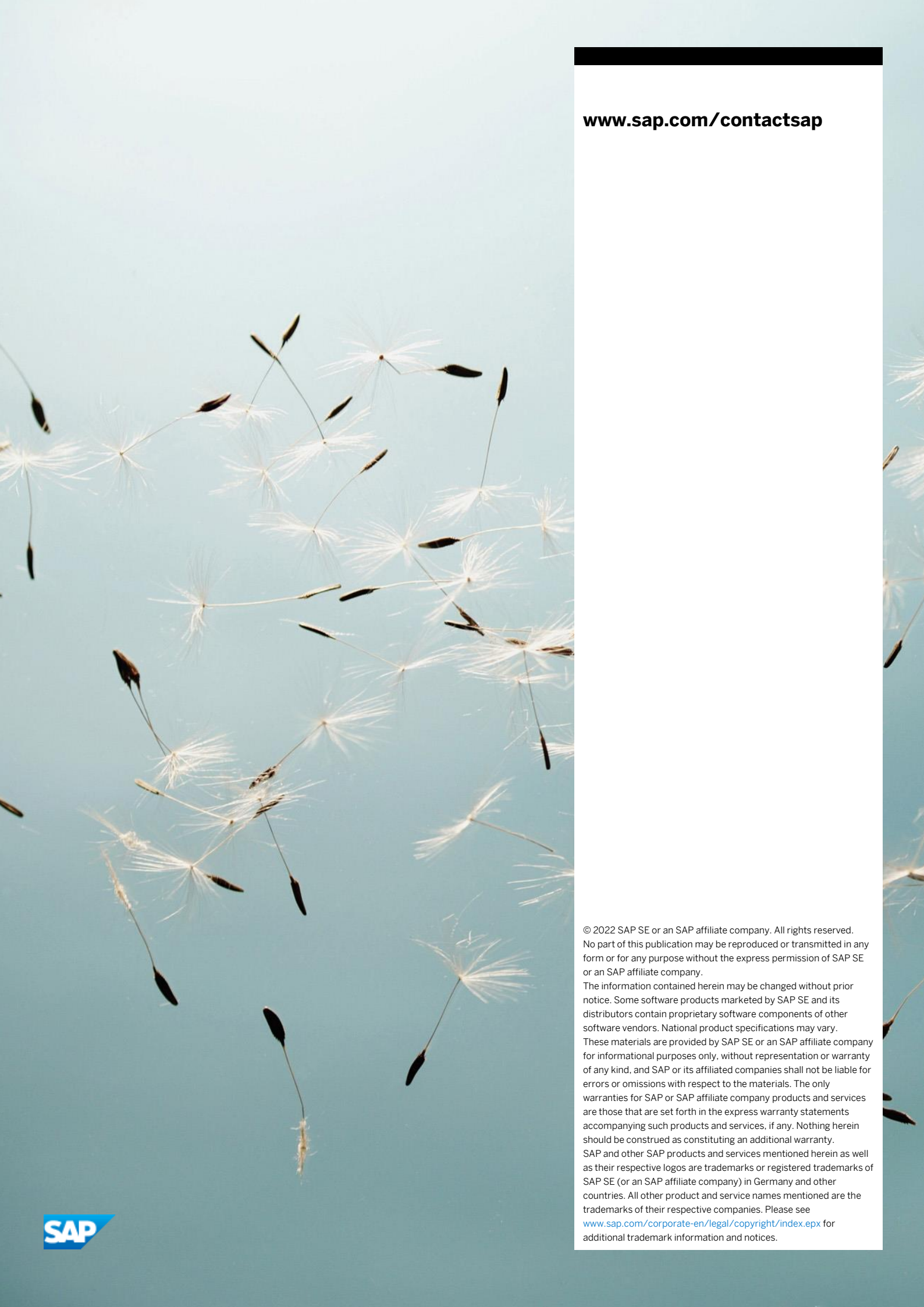
https://test00.aws.tpa-cal-test.com:44301/sap/bc/ui5_ui5/ui2/ushell/shells/abap/FioriLaunchpad.html



For appliances running with FQDN the connect options offered in the user interface go now via FQDN and the external IP addresses. As an exception the RDP connection is still addressed via the internal IP addresses.

In general, the dummy.nodomain resolution via internal IP addresses does still work in addition for all connections.

Note that if you have problems with this feature, you can report an incident within the component: **BC-VCM-CAL**.



www.sap.com/contactsap