SAS® Viya® 3.4 Administration: Multi-tenancy

Multi-tenancy: Overview . . . **2**
- Fundamentals . . . 2
- Administration . . . 2

How To (Provider Administrators) . . . **2**
- Tasks of the Provider Administrator . . . 2
- Onboard Tenants . . . 3
- Manage Tenants . . . 11
- Offboard Tenants . . . 12
- Add Resources to Tenants . . . 15
- Enable Guest Access . . . 15

How To (Tenant Administrators) . . . **16**
- Tasks of the Tenant Administrator . . . 16
- Configure a New Tenant After Onboarding . . . 17
- Tenant Management Interfaces . . . 17

Multi-tenancy: Concepts . . . **17**
- Introducing Multi-tenancy . . . 17
- User Accounts and Passwords . . . 18
- Introducing the CAS Host Groups . . . 19
- Data Separation in Multi-tenancy . . . 19
- Parallel Sets of Groups . . . 20
- Offboarding Tenants . . . 21
- About Multi-tenant Backup and Restore . . . 21

Troubleshooting . . . **21**
- Tenant Administrators Not Added during Onboarding . . . 21
- Tenant Command-Line Interface Can Fail after Onboarding . . . 21
- Onboarding Can Fail with a Log-Watcher Service Error . . . 21
- Unable to Access the Tenant URL . . . 22
- Tenant Remains in an Onboarding State . . . 22
- Tenant Cannot Access Hadoop After Onboarding . . . 22
- Administrator Cannot View Logs for the Provider . . . 22
- sasgpud Error When Running the Onboarding Playbook . . . 22

Multi-tenancy: Overview

Fundamentals

This document applies only to multi-tenant deployments.

Multi-tenant deployments are supported only in the Linux operating environment.

Multi-tenant deployments consist of a *provider* and multiple *tenants*. The provider is a specialized tenant that has the sole purpose of adding, managing, and deleting tenants. The tenants provide data isolation for specified groups of users.

Access to software applications is determined by Identities Service groups and host groups. The groups can be configured to share a single instance of an application across multiple tenants, while maintaining data isolation. The groups can also be configured to support multiple instances of an application, one instance per tenant.

The deployment of multi-tenancy creates the provider. After deployment, administrators create and configure tenants and tenant groups. For more information about multi-tenant deployment, see the *SAS® Viya® 3.4 for Linux: Deployment Guide*.

The process of creating and configuring tenants is known as *onboarding*. Decommissioning and removing tenants is known as *offboarding.*

Administration

Multi-tenant deployments require the assignment of users to the roles of *provider administrator* and *tenant administrator*.

Provider administrators onboard and offboard tenants, configure tenants at the system level, monitor tenant operation, and troubleshoot tenants. For information about provider administrator tasks, see “Tasks of the Provider Administrator” on page 2.

Tenant administrators manage software applications and control data access within a single tenant. The tasks of tenant administrators include the creation of user groups and assignment of permissions to users and groups. For information about tenant administrator tasks, see “Tenant Management Interfaces” on page 17.

To learn more about multi-tenancy, see “Multi-tenancy: Concepts”.

How To (Provider Administrators)

Tasks of the Provider Administrator

The provider-level administrator has additional permissions and responsibilities compared to the tenant administrator. Here are examples of provider-level tasks:

- view or modify deployment resources (Consul key-value pairs, system configuration properties, system component status, and so on)
- modify connection information for the LDAP identity provider
- manage product licenses
- access application and server logs
- perform machine-level monitoring

- modify contents of LDAP
- perform provider-level backup and recovery
- perform tenant management tasks

Onboard Tenants

The process of creating a tenant and making it ready for use is known as *onboarding*. The following sections pertain to onboarding tenants.

Note: You do not have to onboard all tenants at the same time. More tenants can be added later.

Prerequisites for Onboarding

1 Verify that your initial deployment included multi-tenancy.

> **TIP** A simple test is to look at the SAS Environment Manager user interface, when you are signed in as an administrator. If the deployment is multi-tenancy-enabled, the **Tenants** option is visible in the left-navigation bar. If not, then you must re-install with multi-tenancy enabled before you can configure your tenants.

See Enable Multi-tenancy.

Note: When you run the playbook, a multi-tenancy-enabled deployment creates a single tenant with the tenant ID **`provider`**.

2 If you plan to onboard multiple tenants, then you need to tune your operating environment and SAS Viya for performance and scalability. See*SAS Viya Administration: Tuning*.

3 Understand how the LDAP structure is configured for the provider.

- separate LDAP server per tenant
- single LDAP server for all tenants

For more information see "Considerations for Multi-tenancy and LDAP" in *SAS Viya for Linux: Deployment Guide*.

4 Ensure that the zones are configured correctly, as described in Enable Multi-tenancy. For a description of a zone, see zones.

5 The jq package must be installed on any hosts where the command line interface is installed before you begin onboarding. Those hosts are in the **`[CommandLine]`** host group in the inventory file.

If the jq package is not installed on the hosts in the **`[CommandLine]`** host group, then the onboarding playbook fails with the message `jq: command not found`. For more information about the jq package, see "(Optional) Additional Requirement for Multi-tenancy" in *SAS Viya for Linux: Deployment Guide*.

6 The access control list (ACL) package must be installed on any hosts in the **`[ComputeServer]`** host group and the **`[programming]`** host group before you begin onboarding.

If the ACL package is not installed in the two host groups, the onboarding playbook fails with the message `setfacl: command not found`. For more information about the ACL package, see "(Optional) Additional Requirement for Multi-tenancy" in *SAS Viya for Linux: Deployment Guide*.

Perform a Backup

Take a full binary backup before onboarding tenants. See About Default Backup and Binary Backup for more details.

Before taking a backup, check your solution documentation for application-specific instructions.

Determine the Tenant ID

The tenant ID identifies the new tenant in many places, including URLs, the file system, and in the LDAP server configuration. Due to its wide use, the tenant ID must meet the following requirements.

The tenant ID must be unique, 1-16 characters in length, contain only lowercase letters (only a-z in the English alphabet) and numbers, and begin with a letter. The following identities are reserved: *default*, *provider*, *shared*, *sharedservices*, *spre*, *uaa*, *viya*, and any identity beginning with “sas”.

The tenant ID must correspond to a valid LDAP identity for the tenant if you are using a single LDAP server for all tenants. For more information about LDAP identities see Configuration Properties: Reference (Services).

If you are configuring a separate LDAP server for each tenant, then you can use the configuration properties to point to any LDAP location.

To see a list of tenants that have already been configured, run the following command:

```
/opt/sas/viya/home/bin/sas-admin --profile provadmin tenant list
```

To run the previous command, you must have already signed in to SAS Viya at the command line. See “Command-Line Interface: Preliminary Instructions” in *SAS Viya Administration: Using the Command-Line Interfaces*.

In the file <*tenantID*>_vars.yml, replace the **`sas_tenant`** value with the tenant ID.

In this document, everywhere that **`<tenantID>`** appears, substitute the tenant ID value that you chose. For example, if you chose acme, this should be substituted into **`/opt/sas/<tenantID>`** to produce **`/opt/sas/acme`**.

Set Up User Accounts Based on Your LDAP Configuration

Before you onboard a new tenant, you need to set up user accounts in LDAP. The setup task depends on your LDAP configuration.

When your multi-tenant configuration was deployed, LDAP was set up in one of two ways. Your site either uses a single LDAP server for all tenants, or separate LDAP servers, one for each tenant.

To set up user accounts in a configuration that uses a single LDAP server for all tenants, see “Set Up Accounts for Multi-tenant Deployments: Single LDAP Server for All Tenants” in *SAS Viya for Linux: Deployment Guide*.

To set up user accounts when each tenant has a separate LDAP server, see “Set Up Accounts for Multi-tenant Deployments: Separate LDAP Server per Tenant” in *SAS Viya for Linux: Deployment Guide*.

Ensure that there is at least one valid user that can be configured as the initial tenant administrator. For more information see “Set Up Accounts for Multi-tenant Deployments: Separate LDAP Server per Tenant” in *SAS Viya for Linux: Deployment Guide*.

Ensure That Resources Are Sufficient

1. Ensure that you have sufficient host resources to onboard tenants. For more information see “Add Shared Resources across All Tenants”.
2. Identify the resources for the tenant CAS configuration and add resources as needed. See “Add CAS Resources to a Tenant ”.

3 Identify the following resources for the programming run-time environment that is configured per-tenant:
   - SAS Compute Server and Compute Service
   - SAS Launcher and Launcher Service
   - SAS Workspace Server and Object Spawner
   - Embedded web application server
   - SAS/CONNECT Server and Spawner

   For more information see Programming Run-Time Servers.

4 Connect to LDAP each of the hosts identified for the new tenant and for run-time servers.
   - Add tenant members to LDAP.
   - If you use one LDAP server per tenant, then configure the hosts to communicate to the tenant's LDAP server.

Increase Available Disk Space

If additional disk space is needed for a tenant, a provider administrator should increase disk space before onboarding the tenant. To increase disk space, mount the volume at **/opt/sas/<*tenantID*>**.

Set Up a Secondary CAS Controller (Optional)

If you intend to have a secondary CAS controller for your tenant, then both the primary and secondary controller must use a shared file system. For more information, see"Enable a Shared File System" in *SAS Viya for Linux: Deployment Guide*.

Configure the shared file system:

1 Create and configure the directory **/opt/sas/<*tenantID*>/config/data/cas** on both controllers. Where <*tenantID*> is the tenant ID of the tenant that you plan to onboard.

```
sudo mkdir –p /opt/sas/<tenantID>/config/data/cas

sudo chown -R <tenant_admin>:<tenant_admin_group>/opt/sas/<tenantID>/config/data/cas

sudo chmod 0755 /opt/sas/<tenantID>/config/data/cas
```

   Note: The **<tenant_admin>** is the owner of files and directories on the disk as well as the process owner of the tenant-specific services. The **<tenant_admin_group>** defines the primary group to which that tenant administrator belongs.

   > **TIP** The values specified for **<tenant_admin>** and **<tenant_admin_group>** must be the same values that are specified when configuring the vars.yml for the tenant.

   For more information see "Configure the vars.yml file for the Tenant".

2 Mount the shared location on both controllers:

```
sudo mount <source-machine>:<path_to_shared_location> /opt/sas/<tenantID>/config/data/cas
```

   Where <*source-machine*> is the host name of the machine where the files are stored and <*path_to_shared_location*> is the absolute path to the shared location.

Configure the vars.yml file for the Tenant

1 Navigate to the sas_viya_playbook directory on the machine where the playbook was unzipped. Locate the sample_tenant_vars.yml file in the samples directory. Create a copy and put it in the sas_viya_playbook directory. Rename the file to *<tenantID>*_vars.yml.

2 Configure the *<tenantID>*_vars.yml file. When configuring the file:

- If you are configuring for a separate LDAP server per tenant, modify `skip_ldap_config: false` to `skip_ldap_config: true`.

  Note: If you are configuring for a single LDAP server for all tenants, keep `skip_ldap_config: false`.

- Replace the values in the *"< replace me >"* or *< replace me >* with your values. For example, to onboard a tenant with tenant ID of acme, `sas_tenant: "<replace me>"` becomes `sas_tenant: acme`
- Do not edit any other text.
- Any password with a blank space in it must be enclosed in double quotation marks (" ").
- Ensure that host names match those in the inventory.ini file.
- Ensure that user names are those specified in the LDAP server. This value must correspond to a valid LDAP identity for the tenant. For more information see "User Accounts and Passwords".
- Port values are configurable, so ensure that ports are unique for the tenant and available.
- The CAS configuration from the provider is not automatically enabled for the tenant. The administrator needs to determine what CAS configuration is needed for the tenant. See the comments and examples in the sample_tenant_vars.yml file.

> **TIP** This file contains unencrypted passwords for both the sasprovider user and a provider administrator. Restrict access to this file.

3 If you are planning to use a load balancer to increase capacity and reliability, you should set its location in the *<tenantID>*_vars.yml file.

a Open the *<tenantID>*_vars.yml file if it is not already open.

b Locate the `CLUSTER_DEFINITIONS` block of variables. Navigate to the `cas` section.

```
cas:
      port: < replace me >
      httpport: < replace me >
      gcport: 0
      #SERVICESBASEURL: 'https://<tenantID>.loadbalancer.company.com'
#env:
      #CAS_DISK_CACHE: /tmp
      #CAS_VIRTUAL_HOST: '<tenantID>.loadbalancer.company.com'
      #CAS_VIRTUAL_PROTO: 'https'
      #CAS_VIRTUAL_PORT: 443
```

c Remove the example values, and replace them with the values for the load balancer.

Note: Change the values for `SERVICESBASEURL` and `CAS_VIRTUAL_HOST` because the default values for both are not true FQDNs. You are not required to change the values for `CAS_VIRTUAL_PROTO` and `CAS_VIRTUAL_PORT` if the defaults are accurate for your deployment.

If other CAS servers are running on the same host, change the port and httpport to avoid port conflicts.

```
cas:
```

```
    port: 5570
    httpport: 8777
    gcport: 0
    #SERVICESBASEURL: 'https://<fully-qualified-domain-name-of-the-load-balancer>'

env:
   #CAS_DISK_CACHE: /tmp
   CAS_VIRTUAL_HOST:  'fully-qualified-domain-name-of-the-load-balancer'
   CAS_VIRTUAL_PROTO: 'protocol-portion-of-the-URL-for-the-reverse-proxy'
   CAS_VIRTUAL_PORT:  port-where-the-load-balancer-listens-for-incoming-connections
```

Note: You must remove the number sign (#) from all the properties listed, even if the default values for `CAS_VIRTUAL_PROTO` and `CAS_VIRTUAL_PORT` are correct for your deployment.

Run the Playbook

Run the multi-tenancy playbook to onboard the tenant.

```
cd <path_to_playbook>
ansible-playbook -i inventory.ini utility/multi-tenancy.yml -e "@<tenantID>_vars.yml" -vv
```

Here is an example: `"@acme_vars.yml"`.

Note: If any errors occur during onboarding, you can view them in a log file located at **`/opt/sas/viya/config/var/log/multitenant/<tenantID>/tenant_onboard.log`**

Note: Make sure that the **`zones: internal.hostnames:`** defined in your playbook folder **`/roles/consul/files/sitedefault.yml`** is correct. The host name should not include `"\r"` at the end of the line. Here is an example of a zone: `internal.hostnames: "myhostname.sas.com"`.

Multiple entries are separated by a comma (for example, `internal.hostnames: "myhostname.sas.com","mycompanyname.sas.com","mycomputer.sas.com"`).

Configure a Separate LDAP Server per Tenant

If you are configuring a separate LDAP server per tenant, you should have specified `skip_ldap_config='true'` in the <tenantID>_vars.yml file. Now you need to complete these steps.

Note: Only LDAP-based identity providers are supported. You should have basic familiarity with LDAP administration. For more information about the properties that are relevant for this task, see "sas.identities.providers.ldap" in *SAS Viya Administration: Configuration Properties*.

1. Sign in to the proper tenant URL using the appropriate sasprovider user ID and password (which was set within the <tenantID>_vars.yml file). The tenant URL is <tenantID>.<hostname>/SASEnvironmentManager.
2. Select the 🔧 from the side menu to open the Configuration page.
3. On the Configuration page, select **Basic Services** ⇨ **Identities service** from the list of services.
4. To configure user properties, in the **sas.identities.providers.ldap.user** section, click **New Configuration**. In the New Configuration window:
   a. Specify a value for the required **baseDN** field. For the remaining fields, review the default values and make changes as necessary. The default values are appropriate for most sites.

      Note: When using the LDAP protocol, passwords are transmitted over the network as clear-text. To secure the deployment, SAS recommends that you configure encrypted LDAP connections. For more information, see Encrypt LDAP Connections in *Encryption in SAS Viya: Data in Motion*.

      For each property that represents a user-level field in SAS, specify a corresponding property in the LDAP server software.

> **TIP** Consider specifying a custom filter to limit the user accounts that SAS Viya returns from your LDAP server.

b Click **Save**.

5 To configure group properties, in the **sas.identities.providers.ldap.group** section, click **New Configuration**.

a In the New Configuration window, specify a value for the required **baseDN** field. For the remaining fields, review the default values and make changes, as necessary. The default values are appropriate for most sites.

For each property that represents a group-level field in SAS, specify a corresponding property in the LDAP server software.

> **TIP** Consider specifying a custom filter to limit the group accounts that SAS Viya returns from your LDAP server.

b Click **Save**.

6 To configure connection properties, in the **sas.identities.providers.ldap.connection** section, click **New Configuration**.

a In the New Configuration window, specify values for the following required fields: **host**, **password**, **port**, **url**, and **userDN**. For the remaining fields, review the default values and make changes, as necessary. The default values are appropriate for most sites.

b Click **Save**.

7 To verify user and group information, from the SAS Environment Manager side menu, select to open the Users page.

a On the Users page, select **Users** from the list in the toolbar. Your users should appear after a few minutes. It is not necessary to restart any servers or services. Then select **Groups** from the list to display your groups.

b Verify that user and group information is displayed correctly. If not, make any necessary changes to the identities service properties.

8 Add the initial tenant administrator to the SAS Administrators group. At least one tenant administrator must be configured. You can also add more tenant administrators at this time.

a Log on to the SAS Environment Manager.

b Click .

c Select **SAS Administrators**.

d Click to display the Edit Members for SAS Administrators window.

e Select the initial tenant administrator from the list, and click to add the initial tenant administrator to the **Selected Identities** box.

f Click **OK**.

9 Sign in to SAS Environment Manager for the provider tenant, and opt in to the SAS Administrator group.

10 In SAS Environment Manager for the provider, check that the tenant is onboarded.

On the Tenants page, confirm that the new tenant has a status of onboarded.

Understand Your Environment

In a multi-tenant environment, the directory **/opt/sas/<tenantID>** might be created on hosts that are not directly related to the tenant. During tenant onboarding, the directories are created to set up the environment for all hosts assigned to the following host groups, as defined in the inventory.ini file:

- **[ComputeServer]**
- **[programming]**
- **[sas-casserver-primary]**
- **[sas-casserver-secondary]**
- **[sas-casserver-worker]**

However, all hosts assigned to the **[sas-casserver-*]** host groups are not necessarily part of the tenant environment because the CAS roles for the tenant environment are assigned in <tenantID>_vars.yml.

Validate the Tenant

1. In SAS Environment Manager for the tenant, confirm that the intended tenant administrators have been added to the SAS Administrators group.

   a. Sign in to the newly created tenant at *<tenantID>*.*<hostname>*/SASEnvironmentManager using the sasprovider user that you configured in the playbook. For example, if you typically access the software at viya.example.com/SASEnvironmentManager, then for a tenant called *acme* the URL becomes: acme.viya.example.com/SASEnvironmentManager.

   b. Opt in to the SAS Administrators assumable group.

2. Confirm that your intended tenant administrators have been added to the SAS Administrators group. See "View User and Group Information" in *SAS Viya Administration: Identity Management* for more information.

3. Confirm that you can start a SAS Cloud Analytics Services (CAS) session. See "SAS Workspace Servers and SAS Cloud Analytic Services" in *SAS Viya Administration: Programming Run-Time Servers* for more details.

4. Validate that the home directories exist for the tenant and are accessible from all machines.

   Set the **homeDirectory** attribute to the default home directory location for users on the host.

   The provider administrator must create this directory before the user can access SAS Studio.

5. Sign back in to the SAS Environment Manager, and navigate to the Tenants page. In the navigation bar, click . Select the new tenant and view the **Access Policy** setting. If it is not already set to **Open**, set this value to **Open**. This allows members of the associated LDAP configuration for this tenant to access the tenant.

6. Enable the tenant. For more information see "Enable Access to the Tenant".

Configure Lockdown in New Tenants

All tenants, including the provider, run in lockdown mode. In lockdown mode, each user works within a specified subset of SAS access methods and file system paths. The available access methods and paths are known as the tenant's *whitelist*. With appropriate file system configuration, the whitelist provides a useful means of partitioning or isolating the data in each tenant.

The whitelist is implemented by the LOCKDOWN system option and statement. The following macro asserts a default whitelist at the start of each user's SAS session on the tenant's Compute Server:

```
lockdown enable_ams=http email ftp hadoop java;
```

```
lockdown path="CAS_CLIENT_SSL_CA_LIST";
    lockdown path="%sysget(SASCONFIG)/data";
    lockdown path="%sysget(config_home)";
    lockdown path="~";
    lockdown path="%sysget(HOME)";
```

To enhance lockdown mode to include tenant-specific paths, edit the following file on the machine that hosts the [ComputeServer] host group:

```
/opt/sas/<tenantID>/config/etc/workspaceserver/default/autoexec_usermods.sas
```

The file autoexec_usermods.sas is empty by default. The following example shows the contents of an updated autoexec_usermods.sas file. The example adds a list of paths to the whitelist of the acme tenant:

```
filename lockit "/opt/sas/acme/config/lockdown_whitelist";
lockdown file=lockit;
```

Tenants that access the Hadoop file system require whitelist configuration in the autoexec. The whitelist needs to contain the paths of the Hadoop configuration directory and the Hadoop JAR file directory.

To protect the whitelist, consider hiding it.

See Also

- LOCKDOWN system option
- LOCKDOWN statement
- Programming run-time servers

Update Apache Server to Use Custom Certificates

SAS Viya replaces the default self-signed certificate installed with the Apache HTTP Server with a certificate that includes a wildcard of subdomains from the fully qualified domain name of the machine. If you update the Apache HTTP Server to use your own custom certificate, ensure that it contains subject alternate names for each tenant or uses a wildcard for the subdomain. See Update Apache HTTP Server TLS Certificates and Cryptography for more information about how to install a new certificate in the Apache HTTP Server.

Onboarding: Next Steps

To conclude the onboarding process, configure the new tenant and notify the tenant administrator.

If the new tenant runs any of the following software, then configure those applications as described in "Creating Analytic Store Directories in a Multi-Tenant Deployment" in *SAS Viya Administration: Models*:

- SAS Model Manager
- SAS Decision Manager and SAS Intelligent Decisioning

  Note: For SAS Intelligent Decisioning, see also "Properties for Multi-tenancy Environments" in *SAS Intelligent Decisioning: Administrator's Guide*.
- SAS Visual Data Mining and SAS Machine Learning
- SAS Visual Text Analytics

Does your new tenant run the SAS Data Preparation software, and does your site use Cloud Data Exchange? If so, then now is the time to deploy Cloud Data Exchange and register SAS Data Agent to your new tenant. See the *SAS Data Agent for Linux: Deployment Guide* and the *Cloud Data Exchange for SAS Viya: Administrator's Guide*.

After you complete the preceding configuration tasks, the new tenant is ready for further configuration by the tenant administrator. Contact the tenant administrators for your new tenant and provide them with the URL for

SAS Environment Manager: *<tenantID>.<hostname>*/SASEnvironmentManager. Also refer the tenant administrators to "How To (Tenant Administrators)".

Manage Tenants

Introduction

These instructions explain how provider administrators use SAS Environment Manager and a command-line interface to manage tenants in a multi-tenant deployment. Instructions are provided to add resources to tenants, enable tenants, disable tenants, offboard tenants, and onboard a previously offboarded tenant.

To onboard a tenant, see "Onboard Tenants".

Navigation

1 Sign in to SASDrive on the provider tenant.

   If you are using SAS Visual Investigator, sign in to SAS Visual Investigator and proceed to the next step.

   > **TIP** Tenant management is administration *of* tenants. Such administration is a provider-level activity. It is performed in the provider by members of the provider's SAS Administrators group. See "Tasks of the Provider Administrator".

2 In the applications menu (☰), select **Administration** ⇨ **Manage Environment**.

   In the navigation bar, click .

View the Properties of a Tenant

1 On the **Tenants** page, select a row.

2 In the table toolbar, click .

Edit the Properties of a Tenant

1 On the **Tenants** page, select a row.

2 In the table toolbar, click .

3 Modify the tenant's name, description, or access policy, and then click **OK**. Note that the tenant ID cannot be changed.

   Here are details about the **Access policy** values:

Open	causes the tenant to be available to all users to authenticate to the system.
Limited	causes the tenant to be available only to the provider administrator.

View the Status of the Services for a Tenant

1 On the Tenants page, select a row.

2 In the table toolbar, click .

Note: The Services Status window provides a list of all the services for the selected tenant as well as the services' status. When all services have a status of "Onboarded", the tenant is fully onboarded.

Enable Access to the Tenant

1 Access SAS Environment Manager on the provider tenant and assume administrative privileges.

2 On the Tenants pane, set the **Access Policy** to **Open** for the tenant.

All users now have authorization to access the tenant.

Disable Access to the Tenant

1 Access SAS Environment Manager on the provider tenant and assume administrative privileges.

2 On the Tenants pane, set the **Access Policy** to **Limited** for the tenant.

No tenant user or tenant administrator can now sign in to the tenant, but jobs and services continue to run.

Note: Users who have active sessions can continue to work.

Offboard Tenants

Overview

The process of removing a tenant from your system is known as offboarding. You can disable a tenant or you can disable and delete a tenant:

- Disable a tenant to prevent user access, without deleting the tenant from the system. Jobs and services continue to run. Only the provider administrator can log on. To enable a disabled tenant, see "Enable Access to the Tenant".
- Disable and delete a tenant to prevent user access, prevent the execution of jobs and services, and remove the tenant from the system. This is the task that is normally referred to as offboarding. To re-onboard a disabled and deleted tenant, see "Re-Onboarding a Tenant".

Prerequisites for Offboarding

Follow these steps before you offboard a tenant.

1 Check the status of the microservices of the tenant that is to be offboarded. Ensure that all microservices are operational. To view the status of the tenant's microservices, see "View the Status of the Services for a Tenant" on page 11.

2 If the tenant that is to be offboarded includes a secondary (backup) CAS controller, then you must remove the shared location of the shared file system before offboarding. If you do not remove the shared location, then onboarding the same tenant can fail.

3 Is the tenant that you plan to offboard configured for SAS Data Preparation and SAS Data Agent? If so, then you must remove the registrations of all instances of SAS Data Agent from that tenant. To display the instances of SAS Data Agent that are registered to the tenant, query the SAS Data Preparation host as shown in the following syntax and example.

   Command syntax:

```
sas-bootstrap-config catalog services | grep -B 5 data_agent | grep serviceName |
   cut -d':' -f2 | sed s/\"//g | sed s/,//
```

   Command example, with sample output:

```
[sas@da-andsch-cloud bin]$ ./sas-bootstrap-config catalog services |
```

```
   grep -B 5 data_agent | grep serviceName | cut -d':' -f2 | sed s/\"//g | sed s/,//
dagentsrv-default-default
dagentsrv-shared-default
dataagent-2
```

To unregister SAS Data Agent, see "SAS Data Preparation Machine: Unregister SAS Data Agent" in *Cloud Data Exchange for SAS Viya: Administrator's Guide*.

Disable an Onboarded Tenant

Run the disable-tenant playbook:

```
cd <path_to_playbook>
ansible-playbook -i inventory.ini utility/disable-tenant.yml -e "@<tenantID>_vars.yml"
```

For example, `"@<tenantID>_vars.yml"` becomes `"@acme_vars.yml"`.

Disable and Delete an Onboarded Tenant

This is the full offboarding procedure.

1. Take a tenant-specific default and binary backup before offboarding a tenant. For more information see Backup and Restore: Taking a Backup.
2. Navigate to the playbook directory `cd <path_to_playbook>`.
3. Run the offboarding playbook:

   ```
   ansible-playbook -i inventory.ini utility/offboard-tenant.yml -e "@<tenantID>_vars.yml"
   ```

   Replace `<tenantID>` with the actual tenant ID. For example, `"@<tenantID>_vars.yml"` becomes `"@acme_vars.yml"`.
4. Remove the SAS Logon service configuration for this tenant. On the **`[sasdatasvrc]`** host, do the following:

   a. `/opt/sas/viya/home/bin/psql -h localhost -p <port> -U dbmsowner -d SharedServices`

   b. Enter the password for the dbmsowner. For instructions about how to obtain the password, see "SAS Infrastructure Data Server" in *SAS Viya Administration: Infrastructure Servers*.

   c. Run the following SQL commands:

      - `delete from logon_provider.group_membership where member_id in (select id from logon_provider.users where identity_zone_id='<tenantID>');`
      - `delete from logon_provider.user_info where user_id in (select id from logon_provider.users where identity_zone_id='<tenantID>');`
      - `delete from logon_provider.users where identity_zone_id='tenantID';`
      - `delete from logon_provider.group_membership where group_id in (select id from logon_provider.groups where identity_zone_id='<tenantID>');`
      - `delete from logon_provider.groups where identity_zone_id='<tenantID>';`
      - `delete from logon_provider.identity_provider where identity_zone_id='<tenantID>';`
      - `delete from logon_provider.identity_zone where name='<tenantID>';`

   If the databasePerTenant configuration property was specified for sas.multi.tenancy.db.mode during configuration of the provider, run these SQL commands. For more information see "Enable Multi-tenancy" in *SAS Viya for Linux: Deployment Guide*.

- `delete from logon.group_membership where member_id in (select id from logon.users where identity_zone_id='<tenantID>');`
- `delete from logon.user_info where user_id in (select id from logon.users where identity_zone_id='<tenantID>');`
- `delete from logon.users where identity_zone_id='<tenantID>';`
- `delete from logon.group_membership where group_id in (select id from logon.groups where identity_zone_id='<tenantID>');`
- `delete from logon.groups where identity_zone_id='<tenantID>';`
- `delete from logon.identity_provider where identity_zone_id='<tenantID>';`
- `delete from logon.identity_zone where name='<tenantID>';`

5 Disable or remove the tenant-based users. Either remove these users from your LDAP environment or block them with a filter for sssd.

   Access to SAS Studio is controlled by the tenant's host operating environment. In this case, the system administrator should remove tenant users from the operating environment.

6 Remove the home directories of the tenant users. The relevant directories are referred to in the **`homeDirectory`** attribute in LDAP.

7 Remove the DNS mapping for the tenant's subdomain.

The tenant is now offboarded. The tenant logon URL might still be reachable, but no account, including sasprovider, can sign on. This acts as a validation step.

You can run the offboard-tenant playbook after you run the disable-tenant playbook for the same tenant. You can also run the offboard-tenant playbook multiple times if the offboard-tenant playbook fails at an earlier stage after appropriate corrective actions are completed.

Here are additional steps to consider:

- Review any backups for the offboarded tenant. You might want to purge these backups, or store them in case the tenant needs to be re-onboarded at a later date.
- Run binary and default backups. See "About Default Backup and Binary Backup" in *SAS Viya Administration: Backup and Restore* for more details.

  Before taking a backup, check your solution documentation for any backup-specific instructions.

The offboarding process creates a log file at each stage: disable, offboard, and delete. The following three log files are created when the offboarding is complete. If the offboarding process fails, you can view the log files for any errors, as well as the status of the tenant services, at each stage.

- **`/opt/sas/viya/config/var/log/multitenant/<tenantID>/tenant_disable.log`** – created when the disable-tenant playbook is run. This log is also created when the offboard-tenant playbook is run.
- **`/opt/sas/viya/config/var/log/multitenant/<tenantID>/tenant_offboard.log`** – created when the offboard-tenant playbook is run.
- **`/opt/sas/viya/config/var/log/multitenant/<tenantID>/tenant_delete.log`** – created when the tenant is being deleted during the running of the offboard playbook.

Re-Onboarding a Tenant

Before an offboarded tenant can be re-onboarded, all SAS Viya services must be restarted (after the tenant was offboarded). For more information, see "General Servers and Services: Overview" in *SAS Viya Administration: General Servers and Services*.

If the offboarded tenant had data that you want to restore, restore the tenant database content. For more information see "Performing a Restore" in *SAS Viya Administration: Backup and Restore*.

Add Resources to Tenants

Overview

Each new tenant requires resources. Overall, the scaling of resources is no different in a multi-tenant environment than in a standard deployment. When adding tenants to an existing SAS Viya deployment, the system downloads and installs the latest software available from the software repository. Therefore, make sure that you are using a mirror repository. See Create a Mirror Repository for more information.

Add Shared Resources across All Tenants

The service layer, which includes the SAS Configuration Server, SAS Infrastructure Data Server, and the SAS Message Broker, is shared across all tenants. To scale these functions, add resources to the original inventory file and rerun the playbook. Additional services might be needed to support higher load requests. To learn more about the service layer, see the *SAS Viya Administration: Infrastructure Servers*.

Add CAS Resources to a Tenant

Each tenant has its own CAS controller. A single machine can host multiple CAS configurations. SAS recommends using a single CAS controller per machine in a production environment.

To add additional CAS machines before you onboard a tenant:

1. Verify that any new machine that you add meets the requirements that are listed in the "System Requirements" in the *SAS Viya 3.4 Linux: Deployment Guide*.
2. To use an existing host defined in the inventory.ini file from the provider:
   a. Hosts specified for the provider in the **[sas-casserver-primary]**, **[sas-casserver-secondary]**, and **[sas-casserver-worker]** host groups can also be used for CAS roles in any tenant environment, without changes to the inventory.ini file. Changes to inventory.ini are not needed because the required CAS software is already installed in the provider.
   b. Hosts specified for the provider in groups other than the **[sas-casserver-primary]**, **[sas-casserver-secondary]**, and **[sas-casserver-worker]** host groups can be used for CAS roles in any tenant environment. The inventory file must be updated to add these hosts to the **[sas-casserver-primary]** host group. The onboarding process installs the necessary CAS software.
3. If hosts that are not part of the initial deployment are needed for CAS hosts in a tenant, then the inventory.ini file must be updated. In the file, add these hosts to the **[sas-casserver-primary]** host group. The playbook must be executed again in order to install the necessary CAS software. To rerun the playbook:

   ```
   ansible-playbook site.yml
   ```

For more information about the CAS host groups, see "Introducing the CAS Host Groups".

Enable Guest Access

This topic supplements the general information and instructions in "Authentication: Guest Access" in *SAS Viya Administration: Authentication*..

Here are details for a provider who wants to enable guest access:

- Manage the guest-related configuration property (sas.logon.provider.guest) as follows:

Table 1 *Guest-Related Configuration Properties*

Goal	Instructions
Make guest access available to selected tenants.	Instruct each participating tenant administrator to add and enable sas.logon.provider.guest within its environment. Do not set that property in the provider.
Make guest access available to the provider and all tenants.	Add and enable sas.logon.provider.guest in the provider. Clear the **Apply configuration only to this tenant (provider)** check box. Each tenant can opt out from within its own environment.
Make guest access available to the provider and selected tenants.	Add and enable sas.logon.provider.guest in the provider. Leave the **Apply configuration only to this tenant (provider)** check box selected. Each tenant can opt-in from within its own environment

- Run the following command for each participating tenant (and for the provider, if applicable):

```
sas-admin authorization facilitate-guest
```

> **TIP** To target a tenant, specify that tenant's URL in your CLI profile. When you sign in, you must supply credentials that are valid for that tenant (for example, the **sasprovider** user created during onboarding).

- Make sure any necessary host-layer access controls are in place. See "Data Separation in Multi-tenancy".
- Instruct each participating tenant administrator to use SAS Environment Manager to make any additional adjustments to guest access within its own environment.

Here are details for a provider who wants to disable guest access:

- To disable guest access, make sure that the sas.logon.provider.guest property is disabled in each appropriate environment.
- If you want to remove rules and access controls that were added by the facilitate-guest commands, follow the general instructions in each appropriate environment.

How To (Tenant Administrators)

Tasks of the Tenant Administrator

Here are tasks of the tenant administrator:

Create and restore tenant-level backups

Add caslibs

Manage access to data

Manage access to content

Manage access to functionality Manage Access to Functionality

Promote content
Assign users to custom groups
Manage mobile devices
Schedule jobs
Set the default QKB and the default locale

Configure a New Tenant After Onboarding

Configure your new tenant as follows:

1. Access *<tenantID>.<hostname>*/SASEnvironmentManager. Sign in with your credentials. Opt in to the SAS Administrators assumable group. If you are not prompted to opt in, check with your provider-level administrator to ensure that you have been added to the SAS Administrators group.
2. Assign users to custom groups, as needed. For example, you might want to designate additional users as tenant administrators in the SAS Administrators group. Note that such changes apply only within your tenant. See *SAS Viya Administration: Identity Management* for more details.
3. Provide your users with the tenant url: <tenantID>.hostname/SASDrive.

Tenant Management Interfaces

In the following table, the shaded part of each circle is an approximation of the amount of tenant administration functionality that a particular interface exposes. The shading indicates relative coverage.

◔	Tenants page	The enterprise graphical interface in SAS Environment Manager.
●	*Command-line interface*	A simple, scriptable interface. Note that the create, delete, onboard, and offboard commands should not be run from the command line. These commands appear in playbooks, and they should be executed only as part of a play.

Multi-tenancy: Concepts

Introducing Multi-tenancy

In multi-tenancy, a provider manages one or more tenants within a single deployment. The essential characteristics of multi-tenancy are separation and sharing.

Here are key points:

- A multi-tenant environment is established only by running a multi-tenant deployment.

- Each tenant is isolated, with no visibility into other tenants or into the provider. The provider can see all tenants, but cannot access them.
- Many components are shared across tenants. For example, applications are shared across tenants.
- Some components have a dedicated instance for each tenant. For example, each tenant has its own dedicated CAS controller.
- You can add tenants to a multi-tenant environment at any time. See *SAS Viya for Linux: Deployment Guide* for more details.

User Accounts and Passwords

The following user accounts and passwords are required when you onboard tenants.

Table 2 *Multi-tenant User Accounts and Passwords*

Account Name and Group	Description	Purpose
provider_admin	This is the ID of the provider administrator. It can be sasboot, or it can be a valid LDAP user that exists for the provider, as long as that user is a member of the SASAdministrators group.	This is the userid parameter that is used by the onboarding playbook to create the tenant, set its state to onboarding, and create the **sasprovider** user. The provider administrator does not have access to authenticate against an individual tenant.
tenant_provider_pwd	This password is used for the **sasprovider** account. The **sasprovider** identity is known only to SASLogon.	Enables the provider administrator to log on to a specific tenant. When **sasprovider** is authenticated to a tenant, **sasprovider** has unrestricted access within that tenant and cannot be disabled by a tenant administrator.
tenant_admin	This is the ID of the tenant administrator and group. This must be a valid LDAP user that exists within the tenant's organizational unit. During the onboarding process, this userid parameter is automatically added to the tenant's SAS Administrators group only if the value in the **skip_ldap_config** field is set to **`false`**. If the tenant_admin was not automatically added to the SAS Administrators group during onboarding, follow these steps to add it to the tenant: ■ As the provider administrator using the **sasprovider** account, log on to the specific tenant to which you want to add the tenant_admin. ■ Using either the SAS Environment Manager or the sas-identities CLI, add the user to the SASAdministrators group. **Note:** Altering the tenant_admin and the SAS Administrators group for the existing tenant is not supported.	The administrator of a tenant. One or more tenant identities can be declared administrators by adding them to the SAS Administrators group within the tenant. One or more tenant administrators are typically created by the **sasprovider** when a tenant is created.

Introducing the CAS Host Groups

Three CAS host groups specify the hosts that implement Cloud Analytic Services on the provider and on each tenant. To learn how to add new hosts to the host groups, see "Add Resources to Tenants".

The CAS host groups are defined as follows:

- The `[sas-casserver-primary]` host group identifies the single host that runs the CAS controller node on the provider. The CAS controller host is the first host in the [sas-casserver-primary] list in the file inventory.ini. For the tenants, host assignment to all three host groups takes place in the file tenant_vars.yml.
- The `[sas-casserver-secondary]` host group identifies the single host that runs the optional CAS backup controller node on the provider, in the file inventory.ini. The CAS backup controller uses a shared file system to support failover for predefined libraries. For more information about the shared file system, see "Enable a Shared File System" in *SAS Viya for Linux: Deployment Guide*.
- The `[sas-casserver-worker]` host group identifies one or more CAS worker nodes for the provider in inventory.ini.

Data Separation in Multi-tenancy

CAS Access Controls

You do not need to use CAS access controls to separate data across tenants. Caslibs and tables are inherently separated by tenant. Here are details:

- Each tenant has its own CAS server.
- Each CAS server can be accessed only by users from the associated tenant. This restriction is established by the tenantid option.
- Each CAS server has its own list of Superusers.

Host Access Controls

Host access controls separate and isolated data across tenants. Host resources are not inherently separated for per-tenant, isolated use. Without host-layer constraints, each CAS server on a single host can access all of the directories and files on that host. Here are the details:

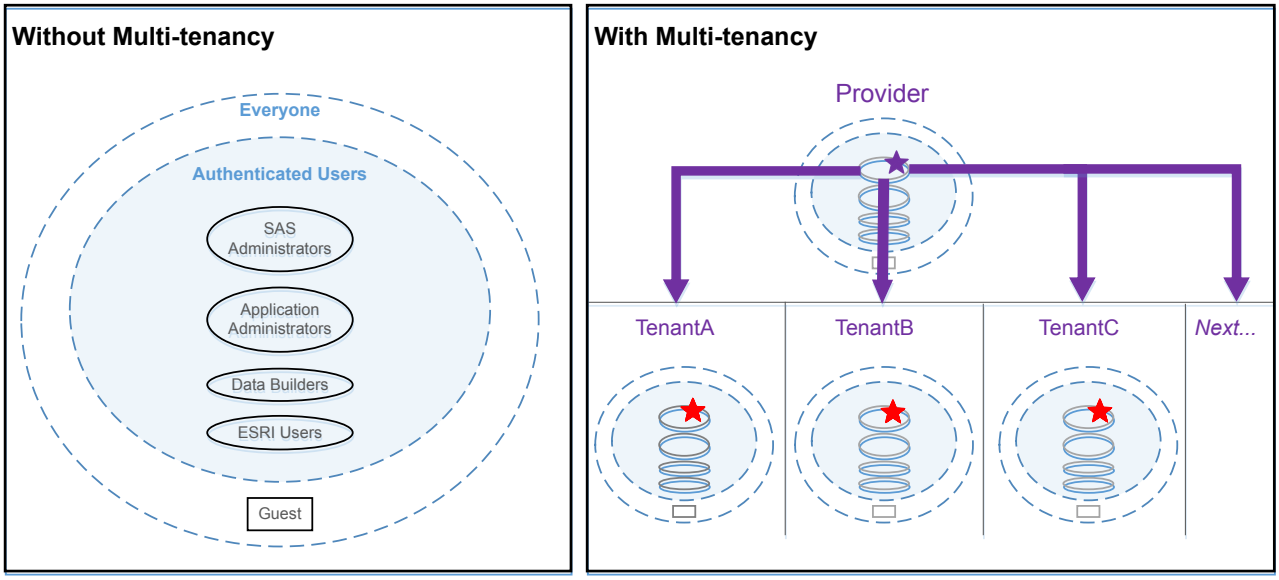
- For visual-interface users who are not members of the CASHostAccountRequired group, host access is under the CAS server's account. Each CAS server runs under a distinct, tenant-specific account. Set host layer access controls so that each server account can access only those directories and files that are appropriate for that tenant.
- For programmers and members of the CASHostAccountRequired group, host access from CAS is under each user's account. Set host layer access controls so that each user's account can access only those directories and files that are appropriate for that user.

> **TIP** You can use a per-server blacklist or whitelist to limit the available host paths for caslib creation. However, Superusers (and any members of the Data role) are not subject to such constraints. See "Paths List" in *SAS Viya Administration: SAS Cloud Analytic Services*.

Parallel Sets of Groups

An identical set of predefined groups and principals exists in the provider and in each tenant. Membership in the provider's SAS Administrators group enables you to perform provider-level tasks, but does not enable you to sign in to any tenant. Membership in a tenant's SAS Administrators group enables you to administer that tenant. The following figure depicts the structure:

Figure 1 *Predefined Groups and Principals*



Here are details about the preceding figure:

- Notice that the provider's groups are the same as the tenants' groups. These are the predefined custom groupsthat are created for each tenant. The provider is implemented as the initial or default tenant. The provider primarily populates and uses its SAS Administrators group. The provider might also populate its other groups for purposes such as validation and reporting.
- The user who is represented by the purple star is the provider and cannot directly access the tenants. Instead, when a tenant is onboarded, a user, **sasprovider**, is created in the SAS Administrators group for the tenant (represented by the red star).
- A tenant administrator can choose to add its own members to its SAS Administrators group.

To isolate the data on the tenant, the provider administrator configures host groups during the onboarding of new tenants. The host groups enforce data isolation by limiting the users of a tenant to the applications and data that are stored and accessed on the specified hosts.

To limit access to applications and data within a new tenant, the provider administrator configures the tenant's LDAP server. Alongside the LDAP permissions, the provider administrator can also update the tenant's predefined custom groups and create new custom groups. The custom groups receive configuration properties that define access control within the new tenant.

After onboarding, the tenant administrator completes the configuration of the custom groups. When access to the tenant's applications and data are fully configured, the tenant administrator informs users that the new tenant is ready for use. The tenant administrator then maintains the custom groups and sends requests to the provider administrator to update LDAP as needed.

Offboarding Tenants

Provider administrators can disable tenants or offboard tenants. Disabling tenants prevents users from accessing applications or data, while allowing operation in applications and services. Offboarding ends the execution of all applications and services in the tenant.

You can onboard a tenant after it has been offboarded.

For more information about offboarding, see "Offboard Tenants".

About Multi-tenant Backup and Restore

Both default and binary backups and restores can be run on individual tenants or on all tenants. Default and binary backups are both necessary components of your backup and recovery plan.

Administrative roles for backup and recovery are defined as follows. Provider administrators can run backups and restores on the provider tenant, on all tenants, or on individual tenants. Provider administrators can run restores on tenants only using backups that were taken by provider administrators.

Tenant administrators can run default backups and restores on their respective tenants. Restores can be run by tenant administrators only from backups that were taken by tenant administrators. Tenant administrators cannot run binary backups or restores.

Specific group memberships for provider and tenant administrators are required to enable backup and restore. For permission requirements and additional information, see *SAS Viya Administration: Backup and Restore*.

Troubleshooting

Tenant Administrators Not Added during Onboarding

If the tenant administrators are not set up correctly when running the tenant_vars.yml play, the provider administrator manually adds them to the tenant's SAS Administrators group. This is done by accessing SAS Environment Manager for the tenant using the appropriate **sasprovider** account. Navigate to the **Users** page, and add the tenant users to the SAS Administrators group.

Tenant Command-Line Interface Can Fail after Onboarding

The tenant CLI can fail if you select the HTTPS scheme as the value of the configuration property provider_endpoint_scheme. To enable the tenant CLI:

1. Edit the inventory.ini file **`sas_viya_playbook/inventory.ini`**.
2. Ensure that the first host in the [CommandLine] group is a host that was also present in any of these groups: [programming], [ComputeServer], or [sas-casserver-*] .
3. Rerun the site.yml playbook.
4. Rerun the onboarding playbook.

Onboarding Can Fail with a Log-Watcher Service Error

The onboarding playbook can fail with a message that contains:

```
fatal: [cas-controller]: FAILED! => {"changed": false, "failed": true,
   "msg": "Unable to start service sas-team2-watch-log-default: Failed
   to start sas-team2-watch-log-default.service: Unit sas-team2-watch-
   log-default.service failed to load: No such file or directory.\n"}
```

The failure occurs when the Unit file for the onboarding init script is not automatically generated.

To resolve the error, rerun the onboarding playbook.

Unable to Access the Tenant URL

If you receive a `404 Not Found` message when attempting to log on to the tenant (for example, <*tenantID*>.hostname/SASEnvironmentManager), and the navigation bar shows <*tenantID*>.hostname/SASLogon, your zones.internal.hostnames property is not configured correctly.

This property must contain the base host name without any tenant prefixes. For example, if tenants are addressed as tenant1.example.com, tenant2.example.com, and so on, the property must contain example.com. Also include any default host names for the provider (localhost is already included).

Also, the host name should not include `"\r"` at the end of the line.

The SAS Logon service and SAS Studio must be restarted when making changes to this property.

Tenant Remains in an Onboarding State

If a tenant stays too long in an onboarding state, log on to SAS Environment Manager (as an administrator on the provider's tenant), and navigate to the **Tenants** page. For the specific tenant in question, select the **Services Status** option, and determine which services have a status of **Onboarding**. For these services, view the appropriate log file, and look for any errors or warnings related to the onboarding process.

Tenant Cannot Access Hadoop After Onboarding

If users in a new tenant cannot access Hadoop, then the tenant's whitelist might need to be updated. See "Configure Lockdown in New Tenants".

The SAS Data Connector for Hadoop must also be configured, as described in "Configure SAS Data Connector to Hadoop" in *SAS Viya for Linux: Deployment Guide*.

Administrator Cannot View Logs for the Provider

After a tenant is onboarded, a tenant administrator is not permitted to view the logs for the provider tenant. Only provider administrators are intended to access the log files of the provider.

sasgpud Error When Running the Onboarding Playbook

When running the onboarding playbook, the following error occurs on cas server controller and worker hosts. This is expected behavior and the error can safely be ignored.

```
TASK [See if the sasgpud service is running]
***********************************************************
fatal: [cas-controller]: FAILED! => {"changed": true, "cmd": ["pgrep", "-x",
"sasgpud"], "delta": "0:00:00.021817", "end": "2018-06-27 08:07:39.043250",
"failed": true, "msg": "non-zero return code", "rc": 1, "start": "2018-06-27
08:07:39.021433", "stderr": "", "stderr_lines": [], "stdout": "",
"stdout_lines": []}
...ignoring
fatal: [cas-worker]: FAILED! => {"changed": true, "cmd": ["pgrep", "-x",
```

"sasgpud"], "delta": "0:00:00.016138", "end": "2018-06-27 08:07:39.083611",
"failed": true, "msg": "non-zero return code", "rc": 1, "start": "2018-06-27
08:07:39.067473", "stderr": "", "stderr_lines": [], "stdout": "",
"stdout_lines": []}
...ignoring