SUSE

Introduction to Ansible Automation for SUSE Linux Enterprise Server for SAP applications 16

WHAT?

Learn about a powerful set of Ansible collections and playbooks that are designed for SAP. This automation codifies best practices, allowing you to build and maintain your SAP landscapes with speed, reliability and consistency.

WHY?

Ansible Automation is essential for SAP environments for organizations to codify and standardize the complex, time-consuming, and high-risk administrative tasks associated with SAP infrastructure and operations.

EFFORT

It takes you up to an hour to read through this article.

GOAL

To transform the management of SAP environments from a complex, error-prone, and time-intensive manual process into a fast, consistent, and fully auditable Infrastructure as Code (IaC) workflow.

REQUIREMENTS

- Understanding of Ansible core and how it works (https://documentation.suse.com/sles/16.0/html/SAP-Ansible/) ↗

- Understanding the architecture of SAP systems

Contents

1 Introduction to Ansible Automation for for SUSE Linux Enterprise Server for SAP applications 16

Ansible Automation is required for SAP landscapes because manually managing the complex, critical and often vast SAP environments is time-consuming, error-prone and struggles to meet modern demands for agility and high availability. Leveraging Ansible allows organizations to implement Infrastructure-as-Code (IaC) principles for SAP, ensuring speed, consistency, and repeatability in vital tasks like provisioning new systems, patching, configuration management and performing complex operational procedures.

This automation minimizes the risk of human error, enables High Availability, significantly accelerates change management and frees up skilled SAP Basis administrators to focus on strategic, high-value work rather than repetitive and manual operations. SUSE provides you with a powerful set of Ansible collections and playbooks designed specifically for SUSE Linux Enterprise Server for SAP applications 16.

2 About the `sles_sap_automation` pattern

Using the SUSE package pattern is recommended because it is the simplest and most reliable method for installing all the required SAP automation components.

By using the pattern, you ensure all required Ansible collections and the playbook packages are installed together, preventing dependency problems. For SUSE Linux Enterprise Server for SAP applications 16, install the `sles_sap_automation` package pattern:

```
> sudo zypper install --type pattern sles_sap_automation
```

This command installs the following packages:

- `ansible-sap-infrastructure`

- `ansible-sap-install`

- `ansible-sap-operations`

- `ansible-sap-playbooks`

> **❗ Important**
>
> Each package contains an Ansible Collection with a curated list of supported Ansible roles. To call out each role in a collection, you must use its fully qualified collection name (FQCN). This tells Ansible exactly where to find the role and prevents any naming conflicts with other collections. For example:

```
---
- name: Ansible Play to install SAP Product
  hosts: all
  tasks:
    - name: Install SAP Product
      ansible.builtin.include_role:
        name: suse.sap_install.sap_swpm
```

3 Understanding the `sles_sap_automation` package pattern

The `sles_sap_automation` package pattern installs four packages: `ansible-sap-install`, `ansible-sap-infrastructure`, `ansible-sap-operations` and `ansible-sap-playbooks`. Each package contains an Ansible Collection with a curated list of supported Ansible roles.

3.1 The `sap_install` collection

The `sap_install` collection installs, configures and manages SAP software on Linux operating systems. This collection covers the following tasks:

- Ensure the operating system is configured, and all required SAP installation media are staged prior to system setup.

- Install the SAP HANA database.

- Install SAP products such as SAP S/4HANA, SAP NetWeaver, etc.

- Enable SAP HANA system replication.

- Configure a High Availability cluster for SAP HANA and ASCS/ERS.

The key roles in this collection include:

- `sap_general_preconfigure`: installs required packages and performs basic OS configuration steps according to applicable SAP notes for installing and running SAP HANA or SAP ABAP Application Platform (formerly known as SAP NetWeaver).

- `sap_hana_preconfigure`: installs additional required packages and performs additional OS configuration steps according to applicable SAP notes for installing and running SAP HANA after the role `sap_general_preconfigure`.

- `sap_netweaver_preconfigure`: installs additional required packages and performs additional OS configuration steps according to applicable SAP notes for installing and running SAP ABAP Application Platform after the role `sap_general_preconfigure`.

- `sap_storage_setup`: prepares a host with the storage requirements of a SAP system (prior to software installation).

- `sap_install_media_detect`: detects and extracts SAP installation media.

- `sap_hana_install`: installs SAP HANA using the SAP HANA database lifecycle manager (HD-BLCM).

- `sap_ha_install_hana_hsr`: configures and enables SAP HANA system replication between two nodes.

- `sap_swpm`: installs various SAP systems installable by SAP Software Provisioning Manager (SW-PM).

- `sap_ha_pacemaker_cluster`: installs and configures Linux Pacemaker High Availability clusters for SAP HANA and SAP NetWeaver systems on various infrastructure platforms.

List of all roles:

```
>  /usr/share/ansible/collections/ansible_collections/suse/sap_install/roles ls
  sap_anydb_install_oracle   sap_ha_install_anydb_ibmdb2   sap_ha_pacemaker_cluster
 sap_hana_preconfigure       sap_maintain_etc_hosts        sap_storage_setup
  sap_general_preconfigure   sap_ha_install_hana_hsr       sap_hana_install
 sap_install_media_detect   sap_netweaver_preconfigure    sap_swpm
```

For more details about the roles and role variables in the `sap_install` collection, refer to the `README.md`, for example:

```
>  /usr/share/ansible/collections/ansible_collections/suse/sap_install/roles/sap_swpm ls
   README.md   defaults   meta   tasks   templates
```

3.2 The `sap_infrastructure` collection

The `sap_infrastructure` collection provides a set of Ansible roles to automate various infrastructure-related tasks for SAP systems. The core focus is on creating and configuring the resources across diverse platforms, including cloud hyperscalers and hypervisors.

This collection covers the following tasks:

- Provision virtual machines on target infrastructure platforms using Ansible. This includes the provisioning of High Availability resources such as routing and load balancing, where applicable.

- Assign temporary virtual IP addresses (VIPs) for application installation before the cluster takes over management.

The key roles in this collection are:

- `sap_vm_provision`: provisions virtual machines to host SAP software.

- `sap_vm_temp_vip`: is a temporary virtual IP (VIP) assigned to OS network interface and will be replaced by the Cluster VIP resource once the cluster is configured.

The following infrastructure platforms are supported:

- AWS EC2 virtual server instance

- Google Cloud Compute Engine virtual machine

- IBM Cloud, Intel virtual server

- IBM Cloud, Power virtual server

- Microsoft Azure virtual machine

- IBM PowerVM virtual machine

List of all roles:

```
>  /usr/share/ansible/collections/ansible_collections/suse/sap_infrastructure/roles ls
   sap_vm_provision   sap_vm_temp_vip
```

For more details about the roles and role variables in the `sap_infrastructure` collection, refer to the `README.md`, for example:

```
>  /usr/share/ansible/collections/ansible_collections/suse/sap_infrastructure/roles/
sap_vm_provision ls
```

```
  PLATFORM_GUIDANCE.md  README.md  defaults  meta  tasks
```

> ❗ **Important**
>
> Since this collection leverages native cloud automation tools, ensure you meet your target platform's specific prerequisites as detailed in the Infrastructure platform guidance (https://github.com/SUSE/community.sap_infrastructure/blob/main/roles/sap_vm_provision/PLATFORM_GUIDANCE.md) ↗. Requirements are not part of the pattern and are not supported.

3.3   The `sap_operations` collection

The `sap_operations` collection executes various day-to-day operation tasks for SAP systems.

This collection covers the following tasks:

- Start, stop and restart of the SAP HANA database server.

- Start, stop and restart of the SAP NetWeaver application server.

- Operate the SAP system using `sapcontrol` and various functions.

- Updating SAP profiles.

List of all roles:

```
>  /usr/share/ansible/collections/ansible_collections/suse/sap_operations/roles ls
   sap_control   sap_profile_update
```

For more details about the roles and role variables in the `sap_operations` collection, refer to the `README.md`, for example:

```
>  /usr/share/ansible/collections/ansible_collections/suse/sap_operations/roles/
sap_control ls
   README.md  defaults  tasks
```

3.4   About `ansible.playbooks_for_sap`

The `ansible.playbooks_for_sap` contains Ansible playbooks for deployment of various SAP software solution scenarios onto different cloud service providers.

To make the playbook easy to use and scalable, the following key principles are used in the design:

- **Modular configuration**: The playbooks use modular configuration, which is a variable system that lets you focus only on the specific values for your environment, eliminating the need to sift through hundreds of unused settings.

- **Brownfield and Greenfield Support**: Flexible by design, the playbooks support both greenfield deployments (creating a landscape from scratch) and brownfield operations (running against existing servers).

- **Interactive mode**: For quick setups or for users who prefer not to manage variable files, an interactive mode is available. This mode will prompt you for all the necessary information, guiding you step-by-step.

- **(Optional) Automated Media Downloads**: If the `community.sap_launchpad` Ansible Collection is installed, the playbooks can automatically download the required SAP installation media for you, saving significant manual effort. This feature requires a valid `SAP S-User` with the necessary download privileges.

The benefits of Ansible playbooks for SAP are:

- The playbooks are designed for simplicity, making them accessible to users across all levels of Ansible experience.

- Easily reconfigurable and extendable, they let you precisely tailor deployments to your needs. For instance, you can customize them for specific SAP versions, integrate monitoring tools, or adapt them to different network topologies.

- Each playbook contains a complete deployment scenario, which ensures consistency and simplifies the process.

- Deploy the same SAP solution across diverse infrastructure including different cloud service providers.

For more details about the `ansible.playbooks_for_sap` collection, refer to the `README.md`:

```
> /usr/share/ansible/playbooks/ansible.playbooks_for_sap ls
  LICENSE  README.md  deploy_scenarios  docs  special_actions
```

and

```
> /usr/share/ansible/playbooks/ansible.playbooks_for_sap/docs ls
```

```
CONTRIBUTING.md  CONTRIBUTORS.md  DEV_EXECUTION_FLOW.md  FAQ.md
GET_STARTED_AZURE_DEVOPS.md  GET_STARTED_MACOS.md  GET_STARTED_WINDOWS.md  README.md
images  sample
```

4 Ansible support coverage

The support matrix for Ansible and Python compatibility:

- **Control node:**

  - Python 3.11 - 3.13

  - ansible-core 2.18

  - Ansible 11

- **Managed node:**

  - Python 3.11 - 3.13

❗ Important

- Python and Ansible versions in the control and managed nodes must be compatible.

- Third-party software is not supported.

- Only versions provided in packages that install into System Python are supported.

- Python Virtual Environment or alternatives like pyenv are not supported.

5 Deploying a High Availability distributed SAP S/4HANA system on AWS

This is a detailed step-by-step procedure to deploy a High Availability and distributed SAP S/4HANA system on Amazon Web Services (AWS). The `ansible-sap-playbooks` package is used to automate infrastructure provisioning and SAP software installation, creating a resilient, scalable and enterprise-grade environment. This procedure uses the pay-as-you-go (PAYG) model for the SUSE operating system, where the subscription cost is included in the AWS instance pricing.

This procedure is intended for system administrators, DevOps engineers and SAP Basis consultants who have a working knowledge of AWS, Ansible and SAP principles.

With this procedure, you can:

- Prepare the control node and the AWS cloud environment for automation.

- Configure Ansible variables for a custom deployment.

- Execute a single playbook to provision and configure the entire SAP S/4HANA system.

- Achieve a fully functional and highly available system ready for post-installation activities.

The resulting High Availability distributed SAP S/4HANA system comprises of the following components:

- Two SAP S/4HANA scale-up servers in a High Availability cluster

- Two ASCS/ERS servers in a High Availability cluster

- One primary application server (PAS)

- One additional application server (AAS)

PROCEDURE 1: DEPLOYMENT IN THE AWS CLOUD ENVIRONMENT

> Provisioning with Ansible requires a pre-existing environment and a service user with the necessary permissions.

1. Prepare your AWS cloud environment with the following:

   - VPC:

     - VPC access control list (ACL)

     - VPC Subnets

     - VPC Security Groups

   - Route 53 (private DNS)

   - Internet Gateway (SNAT)

   - Elastic File System (EFS) Network File System (NFS)

   - Bastion host (AWS EC2 VS)

   - Key Pair for hosts

   For more details on infrastructure prerequisites, refer to the infrastructure prerequisites (https://github.com/SUSE/community.sap_infrastructure/blob/main/roles/sap_vm_provision/PLATFORM_GUIDANCE.md#infrastructure-prerequisites-for-ansible-provisioning-method) ↗.

2. Create a new IAM role or policy appropriate access, using one of the following options:

   - Restricted access, refer to the authorization prerequisites (https://github.com/SUSE/community.sap_infrastructure/blob/main/roles/sap_vm_provision/PLATFORM_GUIDANCE.md#recommended-infrastructure-platform-authorizations) ↗.

   - Full access (not recommended):

     - `arn:aws:iam::aws:policy/AmazonVPCFullAccess`

     - `arn:aws:iam::aws:policy/AmazonEC2FullAccess`

     - `arn:aws:iam::aws:policy/AmazonRoute53FullAccess`

> **Note**

A bastion host is required when provisioning to a private cloud from outside, but it can be ignored if your control node has direct access to your cloud account and VPC. This is accomplished by setting the variable `sap_vm_provision_bastion_execution` to `false`.

3. Prepare the control node.

   a. Install the `sles_sap_automation` pattern, which contains all recommended packages for automation.

   ```
   > sudo  zypper install --type pattern sles_sap_automation
   ```

   b. Verify that the pattern and all the packages are installed.

   ```
   > sudo  zypper info --type pattern sles_sap_automation

      Refreshing service
    'SUSE_Linux_Enterprise_Server_for_SAP_Applications_x86_64'.
      Retrieving repository 'SLE-Product-SLES_SAP-16.0'
    metadata .........................................................................
   [done]
      Building repository 'SLE-Product-SLES_SAP-16.0'
    cache ..............................................................................
   [done]
      Loading repository data...
      Reading installed packages...


      Information for pattern sles_sap_automation:
      -------------------------------------------
      Repository      : SLE-Product-SLES_SAP-16.0
      Name            : sles_sap_automation
      Version         : 16.0-160000.2.2
      Arch            : x86_64
      Vendor          : SUSE LLC <https://www.suse.com/>
      Installed       : Yes
      Visible to User : Yes
      Summary         : automation deployment
      Description     :
         ansible playbooks and roles
      Contents        :
         S  | Name                         | Type     | Dependency
         ---+-----------------------------+---------+-----------
   ```

```
            i  | ansible                  | package | Required
            i  | ansible-linux-system-roles | package | Required
            i  | ansible-sap-infrastructure | package | Required
            i  | ansible-sap-install      | package | Required
            i  | ansible-sap-operations   | package | Required
            i  | ansible-sap-playbooks    | package | Required
           i+  | patterns-sap-automation  | package | Required
           i+  | patterns-sap-base_sap_server | package | Required
```

c. Install the AWS requirements, refer to the pre-requisites (https://github.com/SUSE/community.sap_infrastructure/tree/main/roles/sap_vm_provision#amazon-web-services-aws-prerequisites) ↗.

```
> sudo    ansible-galaxy collection install amazon.aws
```

```
> sudo    zypper install python313-boto3
```

4. Ansible playbooks are installed in `/usr/share/ansible/playbooks`. To prevent changes from being overwritten by future package updates, these files should not be modified directly. For this procedure:

   a. Use the scenario directory `/usr/share/ansible/playbooks/ansible.playbooks_for_sap/deploy_scenarios/sap_s4hana_distributed_ha`.

   b. For simplicity, this procedure stores all customizations in the `/playbooks` directory. Specifically, we will use `/playbooks/S01` as the dedicated directory for our system.

   c. Define the minimal required variables and leave the predefined in place for a simplified configuration.

5. You can encrypt variables for playbooks in different ways to ensure security compliance.

   a. Encrypt all variables in the scenario.

   b. Split variables for reusability and encrypt only what is needed. For example:

   - Cloud credentials and information encrypted in Ansible vault.

   - Scenario passwords encrypted in Ansible vault.

   - Scenario non-sensitive variables without using Ansible vault.

   In this procedure, we use a simplified variant for encrypting whole files.

6. Copy the variable files from the source. Since we are provisioning new servers in AWS, only two variable files are required:

- `ansible_extravars.yml` contains scenario-specific variables.

- `ansible_extravars_aws_ec2_vs.yml` contains platform-specific variables.

```
cp /usr/share/ansible/playbooks/ansible.playbooks_for_sap/deploy_scenarios/
sap_s4hana_distributed_ha/ansible_extravars.yml /playbooks/S01/
```

```
cp /usr/share/ansible/playbooks/ansible.playbooks_for_sap/deploy_scenarios/
sap_s4hana_distributed_ha/ansible_extravars_aws_ec2_vs.yml /playbooks/S01/
```

7. Update the variable file `ansible_extravars.yml`.

a. The following variable defines the provisioning method and platform.

```
sap_vm_provision_iac_type: "ansible"
```

b. The following variable selects the desired topology from the `sap_vm_provision_aws_ec2_vs_host_specifications_dictionary` dictionary.

- Predefined with minimum recommended instances for hosting an SAP system.

- Customizable as you can edit an existing entry or define a new plan.

```
sap_vm_provision_host_specification_plan: "xsmall_256gb"
```

c. The value of the variable `sap_software_product` is the key predefined in the `sap_software_install_dictionary` dictionary. This dictionary follows the same rules as the one above. You can edit an existing entry or create a new one.

```
sap_software_product: "sap_s4hana_2023_distributed"
```

```
sap_install_media_detect_source_directory: "/software"
```

> **!** **Important**
>
> The default execution ignores the list of SAP media files in the `sap_software_install_dictionary` dictionary because the optional package `ansible-sap-launchpad` is not present. This package is available in Package Hub and it allows you to download SAP Media Software when provided with valid S-User credentials with appropriate download authorization.
>
> If this package is not installed, the playbook expects you to have all required files present in the path defined in the `sap_install_media_detect_source_directory` directory. The variables used by `sap_launchpad` role are `sap_id_user` and `sap_id_user_password`.

The password variables are simplified and use the master password. This procedure does not include plan text passwords, so you must define them when updating the variable files.

```
sap_hana_install_use_master_password: "y"  # Use a master password for SAP
 HANA installation (y/n) (String).
```

```
sap_hana_install_master_password: ''  # The master password for SAP HANA
 (String).
```

```
sap_swpm_master_password: ''  # Master password for the SAP system (String).
```

```
sap_swpm_ddic_000_password: '' # Password for the DDIC user in client 000
 (String).
```

```
sap_swpm_db_schema_abap_password: ''  # Password for the ABAP schema user
 (String).
```

```
sap_swpm_db_sidadm_password: ''  # Password for the sid adm user in the
 database (String).
```

```
sap_swpm_db_system_password: ''  # Password for the SYSTEM user in the SAP
 HANA database (String).
```

```
sap_swpm_db_systemdb_password: ''  # Password for the SYSTEM user in the SAP
 HANA system database (String).
```

d. The variables for virtual overlay IP addresses need to follow a specific convention for a given platform.

```
AWS:                    the VIP must be **outside** of any VPC Subnet ranges
 (e.g. 192.168.100.102/32)
```

```
sap_vm_provision_ha_vip_hana_primary: "ENTER_STRING_VALUE_HERE"
```

```
sap_vm_provision_ha_vip_nwas_abap_ascs: "ENTER_STRING_VALUE_HERE"
```

```
sap_vm_provision_ha_vip_nwas_abap_ers: "ENTER_STRING_VALUE_HERE"
```

8. Update the variable file `ansible_extravars_aws_ec2_vs.yml`.

a. The variables for connecting through a bastion host.

```
sap_vm_provision_bastion_user: "ENTER_STRING_VALUE_HERE"  # Bastion user name
 (String).
```

```
sap_vm_provision_bastion_ssh_port: "ENTER_STRING_VALUE_HERE"  # Bastion user
 password (String).
```

```
sap_vm_provision_bastion_public_ip: "ENTER_STRING_VALUE_HERE"  # Public IP of
 the bastion server (String).
```

```
sap_vm_provision_ssh_bastion_private_key_file_path: "ENTER_STRING_VALUE_HERE"
 # Path to bastion server's SSH private key on the execution node (String).
```

```
sap_vm_provision_ssh_host_private_key_file_path: "ENTER_STRING_VALUE_HERE"  #
 Path to target host's SSH private key on the execution node (String).
```

b. The variables for connecting to a cloud environment.

```
sap_vm_provision_aws_access_key: "ENTER_STRING_VALUE_HERE"  # Access key ID
 (String).
```

```
sap_vm_provision_aws_secret_access_key: "ENTER_STRING_VALUE_HERE"  # Secret
 access key (String).
```

```
sap_vm_provision_aws_vpc_availability_zone: "ENTER_STRING_VALUE_HERE"  #
 Availability zone (String).
```

```
sap_vm_provision_aws_vpc_subnet_id: "ENTER_STRING_VALUE_HERE"
```

```
sap_vm_provision_dns_root_domain: "ENTER_STRING_VALUE_HERE"  # Root domain for
 DNS entries (e.g., example.com) (String).
```

```
sap_vm_provision_aws_key_pair_name_ssh_host_public_key:
 "ENTER_STRING_VALUE_HERE"  # SSH Key name in AWS Console (String).
```

```
sap_vm_provision_aws_vpc_sg_names: "ENTER_STRING_VALUE_HERE"  # Comma
 separated list of AWS VPC Service Group names (String).
```

c. The variables for selecting which OS image to use for provisioned instances are defined in the `sap_vm_provision_aws_ec2_vs_host_os_image_dictionary` dictionary, which defines the search pattern for images. In this procedure, a PAYG image is used. SUSE Linux Enterprise Server 16 images will be updated in the dictionary when cloud images are available.

```
sap_vm_provision_aws_ec2_vs_host_os_image: "sles-15-6-sap-ha"
```

d. The scenario specific variables for platform required for configuring High Availability.

```
sap_vm_provision_nfs_mount_point: "ENTER_STRING_VALUE_HERE" # e.g.
 fs-0000.efs.eu-west-2.amazonaws.com:/
```

```
sap_vm_provision_nfs_mount_point_separate_sap_transport_dir:
 "ENTER_STRING_VALUE_HERE" # e.g. fs-0000.efs.eu-west-2.amazonaws.com:/
```

```
sap_vm_provision_nfs_mount_point_type: nfs4  # NFS version (String).
```

```
sap_vm_provision_nfs_mount_point_opts:

 nfsvers=4.1,rsize=1048576,wsize=1048576,hard,timeo=600,retrans=2,noresvport,acl
  # NFS Mount options (String).
```

```
sap_ha_pacemaker_cluster_aws_vip_update_rt: "ENTER_STRING_VALUE_HERE"  # AWS
 Routing Table ID (String).
```

9. Encrypt files with Ansible vault. Files can be encrypted either using a prompt or with a password file. This is easier in larger environments for reusability.
Encryption with a prompt:

```
> sudo ansible-vault encrypt ansible_extravars.yml ansible_extravars_aws_ec2_vs.yml
```

Encryption with a password file, which requires appropriate permissions and protection for security compliance:

```
> sudo ansible-vault encrypt --vault-password-file password.key
  ansible_extravars.yml ansible_extravars_aws_ec2_vs.yml
```

10. Use the playbook directly from `/usr/share/ansible/playbooks/ansible.playbooks_for_sap/deploy_scenarios/sap_s4hana_distributed_ha` without editing it. If you need to adjust the playbook, we recommend copying it outside of the package directory. Execute the Ansible playbook with the Ansible vault key file.

```
> sudo  ansible-playbook /usr/share/ansible/playbooks/ansible.playbooks_for_sap/
deploy_scenarios/sap_s4hana_distributed_ha/ansible_playbook.yml \
  --extra-vars "@./ansible_extravars.yml" \
  --extra-vars "@./ansible_extravars_aws_ec2_vs.yml" \
  --vault-password-file password.key
```

Outcome

You now have a fully operational, High Availability and distributed SAP S/4HANA landscape on AWS. Your new environment includes:

- **A clustered SAP HANA database:** With automated failover to ensure continuous availability.

- **A clustered ASCS/ERS Instance:** Protecting the central services, which are critical for system operation.

- **Multiple application servers:** To distribute the workload and provide scalability.

- **Shared storage:** For binaries and transport files, accessible across the landscape.

Next steps

You can now proceed with post-installation tasks, such as:

- **System Validation:** Performing health checks and verifying the High Availability functionality.

- **SAP Configuration:** Applying initial SAP basis configurations, such as SAP Transport Management System (STMS) and profile parameter tuning.

- **Backup and Recovery:** Implementing a robust backup and recovery strategy for the SAP HANA database and application servers.

- **Monitoring:** Integrating the new landscape with your existing monitoring solutions.

6 Deploying a sandbox SAP BW/4HANA system on GCP

This is a detailed step-by-step procedure to deploy a non-production sandbox SAP BW/4HANA system on Google Cloud Platform (GCP). The `ansible-sap-playbooks` package is used to automate infrastructure provisioning and SAP software installation, resulting in a compact, single-node environment suitable for development, testing or training. This procedures uses the bring-your-own-subscription (BYOS) model for the SUSE operating system.

This procedure is intended for system administrators, DevOps engineers and SAP Basis consultants who have a working knowledge of AWS, Ansible and SAP principles.

With this procedure, you can:

- Prepare the control node and the GCP cloud environment for automation.

- Configure Ansible variables for the sandbox deployment.

- Execute a single playbook to provision and configure the entire SAP system.

- Achieve a functional sandbox system ready for post-installation activities.

The resulting SAP S/4HANA system consists of a single server with the following components:

- One SAP HANA database

- One SAP ABAP SAP Central Services (ASCS)

- One primary application server (PAS)

PROCEDURE 2: DEPLOYMENT ON GCP CLOUD ENVIRONMENT

Provisioning with Ansible requires a pre-existing environment and a service user with the necessary permissions.

1. Prepare your GCP cloud environment with the following:

    - VPC:

        - VPC Subnetwork

    - Compute Firewall

- Compute Router

    - Cloud NAT (SNAT)

- DNS Managed Zone (Private DNS)

- Filestore (NFS) or NFS server

- Bastion host (GCP CE VM)

For more details on infrastructure prerequisites, refer to the infrastructure prerequisites (https://github.com/SUSE/community.sap_infrastructure/blob/main/roles/sap_vm_provision/PLATFORM_GUIDANCE.md#infrastructure-prerequisites-for-ansible-provisioning-method) ↗ .

2. Create a new IAM role or policy with appropriate restricted access. For details, refer to the authorization prerequisites (https://github.com/SUSE/community.sap_infrastructure/blob/main/roles/sap_vm_provision/PLATFORM_GUIDANCE.md#recommended-infrastructure-platform-authorizations) ↗ .

> ## Note
>
> A bastion host is required when provisioning to a private cloud from outside, but it can be ignored if your control node has direct access to your cloud account and VPC. This is accomplished by setting the variable `sap_vm_provision_bastion_execution` to `false`.

3. Prepare the control node.

    a. Install the `sles_sap_automation` pattern, which contains all recommended packages for automation.

    ```
    > sudo  zypper install --type pattern sles_sap_automation
    ```

    b. Verify that the pattern and all the packages are installed.

    ```
    > sudo  zypper info --type pattern sles_sap_automation

       Refreshing service
     'SUSE_Linux_Enterprise_Server_for_SAP_Applications_x86_64'.
       Retrieving repository 'SLE-Product-SLES_SAP-16.0'
     metadata ..........................................................................
    [done]
    ```

```
    Building repository 'SLE-Product-SLES_SAP-16.0'
 cache ..............................................................................
[done]
    Loading repository data...
    Reading installed packages...


    Information for pattern sles_sap_automation:
    --------------------------------------------
    Repository      : SLE-Product-SLES_SAP-16.0
    Name            : sles_sap_automation
    Version         : 16.0-160000.2.2
    Arch            : x86_64
    Vendor          : SUSE LLC <https://www.suse.com/>
    Installed       : Yes
    Visible to User : Yes
    Summary         : automation deployment
    Description     :
        ansible playbooks and roles
    Contents        :
        S  | Name                       | Type     | Dependency
        ---+----------------------------+----------+-----------
        i  | ansible                    | package  | Required
        i  | ansible-linux-system-roles | package  | Required
        i  | ansible-sap-infrastructure | package  | Required
        i  | ansible-sap-install        | package  | Required
        i  | ansible-sap-operations     | package  | Required
        i  | ansible-sap-playbooks      | package  | Required
        i+ | patterns-sap-automation    | package  | Required
        i+ | patterns-sap-base_sap_server | package | Required
```

c. Install the GCP requirements, refer prerequisites (https://github.com/SUSE/community.s-
   ap_infrastructure/tree/main/roles/sap_vm_provision#amazon-web-services-aws-
   prerequisites) ↗ .

```
> sudo   ansible-galaxy collection install google.cloud
```

```
> sudo   zypper install python313-google-auth
```

4. Ansible playbooks are installed in `/usr/share/ansible/playbooks` . To prevent changes from being overwritten by future package updates, these files should not be modified directly. For this procedure:

   a. Use the scenario directory `/usr/share/ansible/playbooks/ansible.playbook-`
      `s_for_sap/deploy_scenarios/sap_bw4hana_sandbox.`

b. For simplicity, this procedure stores all customizations in the `/playbooks` directory. Specifically, we will use `/playbooks/B01` as the dedicated directory for our system.

c. Define the minimal required variables and leave the predefined in place for a simplified configuration.

5. You can encrypt variables for playbooks in different ways to ensure security compliance.

   a. Encrypt all variables in the scenario.

   b. Split variables for reusability and encrypt only what is needed. For example:

      - Cloud credentials and information encrypted in Ansible vault.

      - Scenario passwords encrypted in Ansible vault.

      - Scenario non-sensitive variables without using Ansible vault.

   In this procedure, we use a simplified variant for encrypting whole files.

6. Copy the variable files from the source. Since we are provisioning new servers in GCP, only two variable files are required:

   - `ansible_extravars.yml` contains scenario-specific variables.

   - `ansible_extravars_gcp_ce_vm.yml` contains platform-specific variables.

```
cp /usr/share/ansible/playbooks/ansible.playbooks_for_sap/deploy_scenarios/
sap_bw4hana_sandbox/ansible_extravars.yml /playbooks/B01/
```

```
cp /usr/share/ansible/playbooks/ansible.playbooks_for_sap/deploy_scenarios/
sap_bw4hana_sandbox/ansible_extravars_gcp_ce_vm.yml /playbooks/B01/
```

7. Update the variable file `ansible_extravars.yml`.

   a. The following variable defines the provisioning method.

```
sap_vm_provision_iac_type: "ansible"
```

   b. The following variable selects the desired topology from the `sap_vm_provision_gcp_ce_vm_host_specifications_dictionary` dictionary.

- Predefined with minimum recommended instances for hosting an SAP system.

- Customizable as you can edit an existing entry or define a new plan.

```
sap_vm_provision_host_specification_plan: "xsmall_256gb"
```

c. The value of the variable `sap_software_product` is the key predefined in the `sap_software_install_dictionary` dictionary. This dictionary follows the same rules as the one above. You can edit an existing entry or create a new one.

```
sap_software_product: "sap_bw4hana_2023_sandbox"
```

```
sap_install_media_detect_source_directory: "/software"
```

> **! Important**
>
> The default execution ignores the list of SAP media files in the `sap_software_install_dictionary` dictionary because the optional package `ansible-sap-launchpad` is not present. This package is available in Package Hub and it allows you to download SAP Media Software when provided with valid S-User credentials with appropriate download authorization.
>
> If this package is not installed, the playbook expects you to have all required files present in the path defined in the `sap_install_media_detect_source_directory` directory. The variables used by `sap_launchpad` role are `sap_id_user` and `sap_id_user_password`.

8. The password variables are simplified and use the master password. This procedure does not include plan text passwords, so you must define them when updating the variable files.

```
sap_hana_install_use_master_password: "y"  # Use a master password for SAP HANA
 installation (y/n) (String).
```

```
sap_hana_install_master_password: ''  # The master password for SAP HANA (String).
```

```
sap_swpm_master_password: ''  # Master password for the SAP system (String).
```

```
sap_swpm_ddic_000_password: '' # Password for the DDIC user in client 000 (String).
```

```
sap_swpm_db_schema_abap_password: ''  # Password for the ABAP schema user (String).
```

```
sap_swpm_db_sidadm_password: ''  # Password for the "sid" adm user in the database
  (String).
```

```
sap_swpm_db_system_password: ''  # Password for the SYSTEM user in the SAP HANA
  database (String).
```

```
sap_swpm_db_systemdb_password: ''  # Password for the SYSTEM user in the SAP HANA
  system database (String).
```

9. Update the variable file `ansible_extravars_gcp_ce_vm.yml`.

   a. The variables for connecting through a bastion host.

   ```
   sap_vm_provision_bastion_user: "ENTER_STRING_VALUE_HERE"  # Bastion user name
     (String).
   ```

   ```
   sap_vm_provision_bastion_ssh_port: "ENTER_STRING_VALUE_HERE"  # Bastion user
     password (String).
   ```

   ```
   sap_vm_provision_bastion_public_ip: "ENTER_STRING_VALUE_HERE"  # Public IP of
     the bastion server (String).
   ```

   ```
   sap_vm_provision_ssh_bastion_private_key_file_path: "ENTER_STRING_VALUE_HERE"
     # Path to bastion server's SSH private key on the execution node (String).
   ```

   ```
   sap_vm_provision_ssh_host_private_key_file_path: "ENTER_STRING_VALUE_HERE"  #
     Path to target host's SSH private key on the execution node (String).
   ```

   ```
   sap_vm_provision_ssh_host_public_key_file_path: "ENTER_STRING_VALUE_HERE"  #
     Path to bastion public host key on execution node (String).
   ```

   b. The variables for connecting to a cloud environment.

   ```
   sap_vm_provision_gcp_credentials_json: "ENTER_STRING_VALUE_HERE"  # Path to
     JSON credentials file (String).
   ```

   ```
   sap_vm_provision_gcp_project: "ENTER_STRING_VALUE_HERE"  # Project name
     (String).
   ```

   ```
   sap_vm_provision_gcp_region_zone: "ENTER_STRING_VALUE_HERE"  # Region zone
     (String).
   ```

   ```
   sap_vm_provision_gcp_vpc_name: "ENTER_STRING_VALUE_HERE"  # VPC name (String).
   ```

```
sap_vm_provision_gcp_vpc_subnet_name: "ENTER_STRING_VALUE_HERE"  # VPC Subnet
 name (String).
```

```
sap_vm_provision_dns_root_domain: "ENTER_STRING_VALUE_HERE"  # Root domain for
 DNS entries (e.g., example.com) (String).
```

10. The variables for selecting which OS image to use for provisioned instances are defined in the `sap_vm_provision_gcp_ce_vm_host_os_image_dictionary` dictionary, which defines the search pattern for images. In this procedure, a BYOS image is used. SUSE Linux Enterprise Server 16 images will be updated in the dictionary when cloud images are available.

```
sap_vm_provision_gcp_ce_vm_host_os_image: "sles-15-6-sap-byos"
```

```
sap_vm_provision_os_online_registration_user: "ENTER_STRING_VALUE_HERE"  # User/
Email for SUSEConnect registration (String).
```

```
sap_vm_provision_os_online_registration_passcode:  "ENTER_STRING_VALUE_HERE"  #
 Registration code for SUSEConnect registration (String).
```

11. Encrypt files with Ansible vault. Files can be encrypted either using a prompt or with a password file. This is easier in larger environments for reusability.
Encryption with a prompt:

```
> sudo ansible-vault encrypt ansible_extravars.yml ansible_extravars_gcp_ce_vm.yml
```

Encryption with a password file, which requires appropriate permissions and protection for security compliance:

```
> sudo ansible-vault encrypt --vault-password-file password.key
  ansible_extravars.yml ansible_extravars_gcp_ce_vm.yml
```

12. Use the playbook directly from `/usr/share/ansible/playbooks/ansible.playbooks_for_sap/deploy_scenarios/sap_bw4hana_sandbox` without editing it. If you need to adjust the playbook, we recommend copying it outside of the package directory. Execute the Ansible playbook with the Ansible vault key file.

```
> sudo ansible-playbook /usr/share/ansible/playbooks/ansible.playbooks_for_sap/
deploy_scenarios/sap_bw4hana_sandbox/ansible_playbook.yml \
  --extra-vars "@./ansible_extravars.yml" \
  --extra-vars "@./ansible_extravars_gcp_ce_vm.yml" \
  --vault-password-file password.key
```

Outcome

You now have a fully operational, non-production sandbox SAP BW/4HANA system running on a single virtual machine in GCP.

Your new environment includes:

- **A Single GCP Compute Engine VM:** Hosting all SAP instances.

- **SAP HANA Database:** The underlying database for your BW/4HANA system.

- **SAP ASCS and PAS Instances:** The central services and primary application server are installed on the same host.

Next steps

You can now proceed with post-installation tasks, such as:

- **System Validation:** Perform basic health checks to ensure the SAP system is running correctly.

- **Development and Prototyping:** Begin developing and testing new data models and reports in a safe, isolated environment.

- **SAP Configuration** Apply any necessary post-installation configurations or client copies.

- **Learning and Exploration:** Use the system to explore the features of SAP BW/4HANA.

7 Deploying a sandbox SAP ECC on SAP HANA system on existing hosts

This is a detailed step-by-step procedure to deploy a non-production sandbox SAP ECC on an SAP HANA system on existing hosts. The `ansible-sap-playbooks` package is used to automate infrastructure provisioning and SAP software installation, resulting in a compact, single-node environment suitable for development, testing or training.

This procedure is intended for system administrators, DevOps engineers and SAP Basis consultants who have a working knowledge of AWS, Ansible and SAP principles.

With this procedure, you can:

- Prepare the control node and existing hosts.

- Configure Ansible variables for the sandbox deployment.

- Execute a single playbook to provision and configure the entire SAP system.

- Achieve a fully functional system ready for post-installation activities.

The resulting SAP ECC system consists of a single server with the following components:

- One SAP HANA database

- One SAP ABAP SAP Central Services (ASCS)

- One primary application server (PAS)

PROCEDURE 3: DEPLOYMENT ON EXISTING HOSTS

This procedure assumes you have an existing server or a virtual machine on which you will install the SAP ECC sandbox system. It is a must that you provide this host and ensure it is ready for Ansible automation. It is a requirement to establish a secure and passwordless SSH connection from your Ansible control node to the target host.

1. Create an Ansible inventory file.

   a. Ansible needs to know which host(s) to target. Copy the predefined inventory `/usr/share/ansible/playbooks/ansible.playbooks_for_sap/deploy_scenarios/sap_ecc_hana_sandbox/optional/ansible_inventory_noninteractive.yml` to your working directory `/playbooks/E01/`.

   b. Update the file with the connection details of your hosts. For example:

   ```
   ---

   hana_primary:
     hosts:
       sap-s4hana:
         ansible_host: 192.168.1.100
         ansible_port: 22
         ansible_user: root
         ansible_ssh_private_key_file: "/playbook/E01/hosts_rsa"
   ```

   > 📝 **Note**
   >
   > This group name is used in the example playbook and renaming it would require customizing the playbook to change all `hosts:` entries.

2. Configure passwordless SSH authentication.

For automation, the Ansible control node must be able to connect to the target host as `root` without a password prompt. This is achieved using SSH keys.

> **Note**
>
> For simplicity, this procedure uses `root` login, which is acceptable for a temporary sandbox environment. For production systems, using a dedicated, non-root user is the recommended security practice.

a. Generate an SSH key if you do not have one. Press `Enter` to accept the default location and leave the passphrase empty for passwordless access.

```
# ssh-keygen -t rsa
```

b. Copy the SSH public key to the target host. The easiest way to copy your public key to the target host's `authorized_keys` file is using the `ssh-copy-id` utility. This command prompts you for the `root` password of the target host one last time.

```
# ssh-copy-id root@192.168.1.100
```

3. Verify that Ansible can successfully connect to and gather facts from your target host.

```
> sudo ansible -i ansible_inventory_noninteractive.yml all -m ping
```

A successful connection test shows a ping-pong response.

```
192.168.1.100 | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3.13"
    },
    "changed": false,
    "ping": "pong"
}
```

4. Prepare the control node.

a. Install the `sles_sap_automation` pattern, which contains all recommended packages for automation.

```
> sudo zypper install --type pattern sles_sap_automation
```

b. Verify that the pattern and all the packages are installed.

```
>  sudo   zypper info --type pattern sles_sap_automation

        Refreshing service
 'SUSE_Linux_Enterprise_Server_for_SAP_Applications_x86_64'.
        Retrieving repository 'SLE-Product-SLES_SAP-16.0'
 metadata ...........................................................................
[done]
        Building repository 'SLE-Product-SLES_SAP-16.0'
 cache .............................................................................
[done]
        Loading repository data...
        Reading installed packages...


        Information for pattern sles_sap_automation:
        -------------------------------------------
        Repository      : SLE-Product-SLES_SAP-16.0
        Name            : sles_sap_automation
        Version         : 16.0-160000.2.2
        Arch            : x86_64
        Vendor          : SUSE LLC <https://www.suse.com/>
        Installed       : Yes
        Visible to User : Yes
        Summary         : automation deployment
        Description     :
            ansible playbooks and roles
        Contents        :
            S  | Name                       | Type     | Dependency
            ---+----------------------------+----------+-----------
            i  | ansible                    | package  | Required
            i  | ansible-linux-system-roles | package  | Required
            i  | ansible-sap-infrastructure | package  | Required
            i  | ansible-sap-install        | package  | Required
            i  | ansible-sap-operations     | package  | Required
            i  | ansible-sap-playbooks      | package  | Required
            i+ | patterns-sap-automation    | package  | Required
            i+ | patterns-sap-base_sap_server | package | Required
```

5. Ansible playbooks are installed in `/usr/share/ansible/playbooks` . To prevent changes from being overwritten by future package updates, these files should not be modified directly. For this procedure:

   a. Use the scenario directory `/usr/share/ansible/playbooks/ansible.playbooks_for_sap/deploy_scenarios/sap_ecc_hana_sandbox`.

b. For simplicity, this procedure stores all customizations in the `/playbooks` directory. Specifically, we will use `/playbooks/E01` as the dedicated directory for our system.

c. Define the minimal required variables and leave the predefined in place for a simplified configuration.

> **❗ Important**
>
> Ansible playbooks for SAP are designed to skip provisioning when existing hosts are used, but the remaining tasks are all retained. This means that there will be some variables that are part of provisioning, but they can be used even for existing hosts. For example, the `sap_vm_provision_existing_hosts_host_specifications_dictionary` dictionary will not provision new infrastructure, but it will be used to configure storage if defined.

6. You can encrypt variables for playbooks in different ways to ensure security compliance.

a. Encrypt all variables in the scenario.

b. Split variables for reusability and encrypt only what is needed. For example:

- Cloud credentials and information encrypted in Ansible vault.

- Scenario passwords encrypted in Ansible vault.

- Scenario non-sensitive variables without using Ansible vault.

In this procedure, we use a simplified variant for encrypting whole files.

7. Copy the variable files from the source. Since we are using existing hosts, only two variable files are required:

- `ansible_extravars.yml` contains scenario-specific variables.

- `optional/ansible_extravars_existing_hosts.yml` contains platform-specific variables.

```
cp /usr/share/ansible/playbooks/ansible.playbooks_for_sap/deploy_scenarios/
sap_ecc_hana_sandbox/ansible_extravars.yml /playbooks/E01/
```

```
cp /usr/share/ansible/playbooks/ansible.playbooks_for_sap/deploy_scenarios/
sap_ecc_hana_sandbox/optional/ansible_extravars_existing_hosts.yml /playbooks/E01/
```

8. Update the variable file `ansible_extravars.yml`.

   a. s the provisioning method.

   ```
   sap_vm_provision_iac_type: "ansible"
   ```

   b. The following variable selects the desired topology from the `sap_vm_provision_exist-ing_hosts_host_specifications_dictionary` dictionary.

      - Predefined with minimum recommended instances for hosting an SAP system.

      - Customizable as you can edit an existing entry or define a new plan.

      ```
      sap_vm_provision_host_specification_plan: "xsmall_256gb"
      ```

   c. The value of the variable `sap_software_product` is the key predefined in the `sap_soft-ware_install_dictionary` dictionary. This dictionary follows the same rules as the one above. You can edit an existing entry or create a new one.

      ```
      sap_software_product: "sap_ecc6_ehp8_hana_sandbox"
      ```

      ```
      sap_install_media_detect_source_directory: "/software"
      ```

      > ❗ **Important**
      >
      > The default execution ignores the list of SAP media files in the `sap_software_in-stall_dictionary` dictionary because the optional package `ansible-sap-launchpad` is not present. This package is available in Package Hub and it allows you to download SAP Media Software when provided with valid S-User credentials with appropriate download authorization.
      >
      > If this package is not installed, the playbook expects you to have all required files present in the path defined in the `sap_install_media_detect_source_direc-tory` directory. The variables used by `sap_launchpad` role are `sap_id_user` and `sap_id_user_password`.

9. The password variables are simplified and use the master password. This procedure does not include plan text passwords, so you must define them when updating the variable files.

```
sap_hana_install_use_master_password: "y"  # Use a master password for SAP HANA
 installation (y/n) (String).
```

```
sap_hana_install_master_password: ''  # The master password for SAP HANA (String).
```

```
sap_swpm_master_password: ''  # Master password for the SAP system (String).
```

```
sap_swpm_ddic_000_password: '' # Password for the DDIC user in client 000 (String).
```

```
sap_swpm_db_schema_abap_password: ''  # Password for the ABAP schema user (String).
```

```
sap_swpm_db_sidadm_password: ''  # Password for the "sid" adm user in the database
 (String).
```

```
sap_swpm_db_system_password: ''  # Password for the SYSTEM user in the SAP HANA
 database (String).
```

```
sap_swpm_db_systemdb_password: ''  # Password for the SYSTEM user in the SAP HANA
 system database (String).
```

10. Update the variable file `ansible_extravars_existing_hosts.ym`.

   - The variables for connecting to existing hosts.

     ```
     # Path to target host's SSH private key on the execution node (String).
     # This SSH key has to be added to authorized_keys on managed node.
     sap_vm_provision_ssh_host_private_key_file_path: "ENTER_STRING_VALUE_HERE"
     ```

     > **!** Important
     >
     > Ansible playbooks for SAP use the Ansible fact `ansible_domain`, which requires
     > a valid `/etc/hosts` configuration on your existing hosts with FQDN to obtain the
     > domain name.

11. Encrypt files with Ansible vault. Files can be encrypted either using a prompt or with a password
    file. This is easier in larger environments for reusability.
    Encryption with a prompt:

    ```
    > sudo ansible-vault encrypt ansible_extravars.yml
      ansible_extravars_existing_hosts.yml
    ```

Encryption with a password file, which requires appropriate permissions and protection for security compliance:

```
> sudo ansible-vault encrypt --vault-password-file password.key
  ansible_extravars.yml ansible_extravars_existing_hosts.yml
```

12. Use the playbook directly from `usr/share/ansible/playbooks/ansible.playbooks_for_sap/deploy_scenarios/sap_ecc_hana_sandbox` without editing it. If you need to adjust the playbook, we recommend copying it outside of the package directory. Execute the Ansible playbook with the Ansible vault key file.

```
> sudo  ansible-playbook /usr/share/ansible/playbooks/ansible.playbooks_for_sap/
deploy_scenarios/sap_ecc_hana_sandbox/ansible_playbook.yml \
        --extra-vars "@./ansible_extravars.yml" \
        --extra-vars "@./ansible_extravars_existing_hosts.yml" \
        --vault-password-file password.key \
        --inventory ansible_inventory_noninteractive.yml
```

Outcome

You now have a fully operational, non-production SAP ECC on an SAP HANA sandbox system installed on your existing host.

Your new sandbox environment includes:

- **SAP ECC 6.0 EHP8:** The core application is installed and ready for use.

- **SAP HANA database:** The system is running on an SAP HANA database.

- **Single-node architecture**: The HANA database, ASCS and PAS instances are all running on the provided single host.

Next steps

You can now proceed with post-installation tasks, such as:

- **System Validation:** Log in to the SAP GUI, run basic transaction codes like `SM50` (Process Overview) or `ST22` (ABAP Runtime Errors) to ensure the system is operational.

- **Initial Configuration:** Perform any required basis configurations, such as setting up the SAP Transport Management System (STMS) or applying custom profile parameters via RZ10.

- **Development and Customization:** Begin ABAP development, or use transaction code `SPRO` to start system customization.

- **Learning and Exploration:** Use the system to explore standard SAP ECC modules and functionality in a safe, isolated environment.

8 For more information

Refer to the following resources:

- Introduction to Ansible Core https://documentation.suse.com/sles/16.0/html/SAP-Ansible/ ↗.

- Ansible Linux System Roles https://documentation.suse.com/sles/16.0/html/SAP-ansible-roles/ ↗.

- Documentation of open source Ansible playbooks for the deployment of various SAP software solutions: https://github.com/SUSE/community.sap_infrastructure/blob/main/README.md ↗

9 Legal Notice

A GNU Free Documentation License

Copyright (C) 2000, 2001, 2002 Free Software Foundation, Inc. 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

0. PREAMBLE

The purpose of this License is to make a manual, textbook, or other functional and useful document "free" in the sense of freedom: to assure everyone the effective freedom to copy and redistribute it, with or without modifying it, either commercially or non-commercially. Secondarily, this License preserves for the author and publisher a way to get credit for their work, while not being considered responsible for modifications made by others.

This License is a kind of "copyleft", which means that derivative works of the document must themselves be free in the same sense. It complements the GNU General Public License, which is a copyleft license designed for free software.

We have designed this License to use it for manuals for free software, because free software needs free documentation: a free program should come with manuals providing the same freedoms that the software does. But this License is not limited to software manuals; it can be used for any textual work, regardless of subject matter or whether it is published as a printed book. We recommend this License principally for works whose purpose is instruction or reference.

1. APPLICABILITY AND DEFINITIONS

This License applies to any manual or other work, in any medium, that contains a notice placed by the copyright holder saying it can be distributed under the terms of this License. Such a notice grants a world-wide, royalty-free license, unlimited in duration, to use that work under the conditions stated herein. The "Document", below, refers to any such manual or work. Any member of the public is a licensee, and is addressed as "you". You accept the license if you copy, modify or distribute the work in a way requiring permission under copyright law.

A "Modified Version" of the Document means any work containing the Document or a portion of it, either copied verbatim, or with modifications and/or translated into another language.

A "Secondary Section" is a named appendix or a front-matter section of the Document that deals exclusively with the relationship of the publishers or authors of the Document to the Document's overall subject (or to related matters) and contains nothing that could fall directly within that overall subject. (Thus, if the

Document is in part a textbook of mathematics, a Secondary Section may not explain any mathematics.) The relationship could be a matter of historical connection with the subject or with related matters, or of legal, commercial, philosophical, ethical or political position regarding them.

The "Invariant Sections" are certain Secondary Sections whose titles are designated, as being those of Invariant Sections, in the notice that says that the Document is released under this License. If a section does not fit the above definition of Secondary then it is not allowed to be designated as Invariant. The Document may contain zero Invariant Sections. If the Document does not identify any Invariant Sections then there are none.

The "Cover Texts" are certain short passages of text that are listed, as Front-Cover Texts or Back-Cover Texts, in the notice that says that the Document is released under this License. A Front-Cover Text may be at most 5 words, and a Back-Cover Text may be at most 25 words.

A "Transparent" copy of the Document means a machine-readable copy, represented in a format whose specification is available to the general public, that is suitable for revising the document straightforwardly with generic text editors or (for images composed of pixels) generic paint programs or (for drawings) some widely available drawing editor, and that is suitable for input to text formatters or for automatic translation to a variety of formats suitable for input to text formatters. A copy made in an otherwise Transparent file format whose markup, or absence of markup, has been arranged to thwart or discourage subsequent modification by readers is not Transparent. An image format is not Transparent if used for any substantial amount of text. A copy that is not "Transparent" is called "Opaque".

Examples of suitable formats for Transparent copies include plain ASCII without markup, Texinfo input format, LaTeX input format, SGML or XML using a publicly available DTD, and standard-conforming simple HTML, PostScript or PDF designed for human modification. Examples of transparent image formats include PNG, XCF and JPG. Opaque formats include proprietary formats that can be read and edited only by proprietary word processors, SGML or XML for which the DTD and/or processing tools are not generally available, and the machine-generated HTML, PostScript or PDF produced by some word processors for output purposes only.

The "Title Page" means, for a printed book, the title page itself, plus such following pages as are needed to hold, legibly, the material this License requires to appear in the title page. For works in formats which do not have any title page as such, "Title Page" means the text near the most prominent appearance of the work's title, preceding the beginning of the body of the text.

A section "Entitled XYZ" means a named subunit of the Document whose title either is precisely XYZ or contains XYZ in parentheses following text that translates XYZ in another language. (Here XYZ stands for a specific section name mentioned below, such as "Acknowledgements", "Dedications", "Endorsements", or "History".) To "Preserve the Title" of such a section when you modify the Document means that it remains a section "Entitled XYZ" according to this definition.

The Document may include Warranty Disclaimers next to the notice which states that this License applies to the Document. These Warranty Disclaimers are considered to be included by reference in this License, but only as regards disclaiming warranties: any other implication that these Warranty Disclaimers may have is void and has no effect on the meaning of this License.

2. VERBATIM COPYING

You may copy and distribute the Document in any medium, either commercially or non-commercially, provided that this License, the copyright notices, and the license notice saying this License applies to the Document are reproduced in all copies, and that you add no other conditions whatsoever to those of this License. You may not use technical measures to obstruct or control the reading or further copying of the copies you make or distribute. However, you may accept compensation in exchange for copies. If you distribute a large enough number of copies you must also follow the conditions in section 3.

You may also lend copies, under the same conditions stated above, and you may publicly display copies.

3. COPYING IN QUANTITY

If you publish printed copies (or copies in media that commonly have printed covers) of the Document, numbering more than 100, and the Document's license notice requires Cover Texts, you must enclose the copies in covers that carry, clearly and legibly, all these Cover Texts: Front-Cover Texts on the front cover, and Back-Cover Texts on the back cover. Both covers must also clearly and legibly identify you as the publisher of these copies. The front cover must present the full title with all words of the title equally prominent and visible. You may add other material on the covers in addition. Copying with changes limited to the covers, as long as they preserve the title of the Document and satisfy these conditions, can be treated as verbatim copying in other respects.

If the required texts for either cover are too voluminous to fit legibly, you should put the first ones listed (as many as fit reasonably) on the actual cover, and continue the rest onto adjacent pages.

If you publish or distribute Opaque copies of the Document numbering more than 100, you must either include a machine-readable Transparent copy along with each Opaque copy, or state in or with each Opaque copy a computer-network location from which the general network-using public has access to download using public-standard network protocols a complete Transparent copy of the Document, free of added material. If you use the latter option, you must take reasonably prudent steps, when you begin distribution of Opaque copies in quantity, to ensure that this Transparent copy will remain thus accessible at the stated location until at least one year after the last time you distribute an Opaque copy (directly or through your agents or retailers) of that edition to the public.

It is requested, but not required, that you contact the authors of the Document well before redistributing any large number of copies, to give them a chance to provide you with an updated version of the Document.

4. MODIFICATIONS

You may copy and distribute a Modified Version of the Document under the conditions of sections 2 and 3 above, provided that you release the Modified Version under precisely this License, with the Modified Version filling the role of the Document, thus licensing distribution and modification of the Modified Version to whoever possesses a copy of it. In addition, you must do these things in the Modified Version:

A. Use in the Title Page (and on the covers, if any) a title distinct from that of the Document, and from those of previous versions (which should, if there were any, be listed in the History section of the Document). You may use the same title as a previous version if the original publisher of that version gives permission.

B. List on the Title Page, as authors, one or more persons or entities responsible for authorship of the modifications in the Modified Version, together with at least five of the principal authors of the Document (all of its principal authors, if it has fewer than five), unless they release you from this requirement.

C. State on the Title page the name of the publisher of the Modified Version, as the publisher.

D. Preserve all the copyright notices of the Document.

E. Add an appropriate copyright notice for your modifications adjacent to the other copyright notices.

F. Include, immediately after the copyright notices, a license notice giving the public permission to use the Modified Version under the terms of this License, in the form shown in the Addendum below.

G. Preserve in that license notice the full lists of Invariant Sections and required Cover Texts given in the Document's license notice.

H. Include an unaltered copy of this License.

I. Preserve the section Entitled "History", Preserve its Title, and add to it an item stating at least the title, year, new authors, and publisher of the Modified Version as given on the Title Page. If there is no section Entitled "History" in the Document, create one stating the title, year, authors, and publisher of the Document as given on its Title Page, then add an item describing the Modified Version as stated in the previous sentence.

J. Preserve the network location, if any, given in the Document for public access to a Transparent copy of the Document, and likewise the network locations given in the Document for previous versions it was based on. These may be placed in the "History" section. You may omit a network location for a work that was published at least four years before the Document itself, or if the original publisher of the version it refers to gives permission.

K. For any section Entitled "Acknowledgements" or "Dedications", Preserve the Title of the section, and preserve in the section all the substance and tone of each of the contributor acknowledgements and/or dedications given therein.

L. Preserve all the Invariant Sections of the Document, unaltered in their text and in their titles. Section numbers or the equivalent are not considered part of the section titles.

M. Delete any section Entitled "Endorsements". Such a section may not be included in the Modified Version.

N. Do not retitle any existing section to be Entitled "Endorsements" or to conflict in title with any Invariant Section.

O. Preserve any Warranty Disclaimers.

If the Modified Version includes new front-matter sections or appendices that qualify as Secondary Sections and contain no material copied from the Document, you may at your option designate some or all of these sections as invariant. To do this, add their titles to the list of Invariant Sections in the Modified Version's license notice. These titles must be distinct from any other section titles.

You may add a section Entitled "Endorsements", provided it contains nothing but endorsements of your Modified Version by various parties--for example, statements of peer review or that the text has been approved by an organization as the authoritative definition of a standard.

You may add a passage of up to five words as a Front-Cover Text, and a passage of up to 25 words as a Back-Cover Text, to the end of the list of Cover Texts in the Modified Version. Only one passage of Front-Cover Text and one of Back-Cover Text may be added by (or through arrangements made by) any one entity. If the Document already includes a cover text for the same cover, previously added by you or by arrangement made by the same entity you are acting on behalf of, you may not add another; but you may replace the old one, on explicit permission from the previous publisher that added the old one.

The author(s) and publisher(s) of the Document do not by this License give permission to use their names for publicity for or to assert or imply endorsement of any Modified Version.

5. COMBINING DOCUMENTS

You may combine the Document with other documents released under this License, under the terms defined in section 4 above for modified versions, provided that you include in the combination all of the Invariant Sections of all of the original documents, unmodified, and list them all as Invariant Sections of your combined work in its license notice, and that you preserve all their Warranty Disclaimers.

The combined work need only contain one copy of this License, and multiple identical Invariant Sections may be replaced with a single copy. If there are multiple Invariant Sections with the same name but different contents, make the title of each such section unique by adding at the end of it, in parentheses, the name of the original author or publisher of that section if known, or else a unique number. Make the same adjustment to the section titles in the list of Invariant Sections in the license notice of the combined work.

In the combination, you must combine any sections Entitled "History" in the various original documents, forming one section Entitled "History"; likewise combine any sections Entitled "Acknowledgements", and any sections Entitled "Dedications". You must delete all sections Entitled "Endorsements".

6. COLLECTIONS OF DOCUMENTS

You may make a collection consisting of the Document and other documents released under this License, and replace the individual copies of this License in the various documents with a single copy that is included in the collection, provided that you follow the rules of this License for verbatim copying of each of the documents in all other respects.

You may extract a single document from such a collection, and distribute it individually under this License, provided you insert a copy of this License into the extracted document, and follow this License in all other respects regarding verbatim copying of that document.

7. AGGREGATION WITH INDEPENDENT WORKS

A compilation of the Document or its derivatives with other separate and independent documents or works, in or on a volume of a storage or distribution medium, is called an "aggregate" if the copyright resulting from the compilation is not used to limit the legal rights of the compilation's users beyond what the individual works permit. When the Document is included in an aggregate, this License does not apply to the other works in the aggregate which are not themselves derivative works of the Document.

If the Cover Text requirement of section 3 is applicable to these copies of the Document, then if the Document is less than one half of the entire aggregate, the Document's Cover Texts may be placed on covers that bracket the Document within the aggregate, or the electronic equivalent of covers if the Document is in electronic form. Otherwise they must appear on printed covers that bracket the whole aggregate.

8. TRANSLATION

Translation is considered a kind of modification, so you may distribute translations of the Document under the terms of section 4. Replacing Invariant Sections with translations requires special permission from their copyright holders, but you may include translations of some or all Invariant Sections in addition to the original versions of these Invariant Sections. You may include a translation of this License, and all the license notices in the Document, and any Warranty Disclaimers, provided that you also include the original English version of this License and the original versions of those notices and disclaimers. In case of a disagreement between the translation and the original version of this License or a notice or disclaimer, the original version will prevail.

If a section in the Document is Entitled "Acknowledgements", "Dedications", or "History", the requirement (section 4) to Preserve its Title (section 1) will typically require changing the actual title.

9. TERMINATION

You may not copy, modify, sublicense, or distribute the Document except as expressly provided for under this License. Any other attempt to copy, modify, sublicense or distribute the Document is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

10. FUTURE REVISIONS OF THIS LICENSE

The Free Software Foundation may publish new, revised versions of the GNU Free Documentation License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. See https://www.gnu.org/copyleft/ ↗ .

Each version of the License is given a distinguishing version number. If the Document specifies that a particular numbered version of this License "or any later version" applies to it, you have the option of following the terms and conditions either of that specified version or of any later version that has been published (not as a draft) by the Free Software Foundation. If the Document does not specify a version number of this License, you may choose any version ever published (not as a draft) by the Free Software Foundation.

ADDENDUM: How to use this License for your documents

```
Copyright (c) YEAR YOUR NAME.
```

If you have Invariant Sections, Front-Cover Texts and Back-Cover Texts, replace the "with...Texts." line with this:

```
with the Invariant Sections being LIST THEIR TITLES, with the
Front-Cover Texts being LIST, and with the Back-Cover Texts being LIST.
```

If you have Invariant Sections without Cover Texts, or some other combination of the three, merge those two alternatives to suit the situation.

If your document contains nontrivial examples of program code, we recommend releasing these examples in parallel under your choice of free software license, such as the GNU General Public License, to permit their use in free software.