Privileged Identity Management for Google Compute Engine Linux VM Instances

Overview

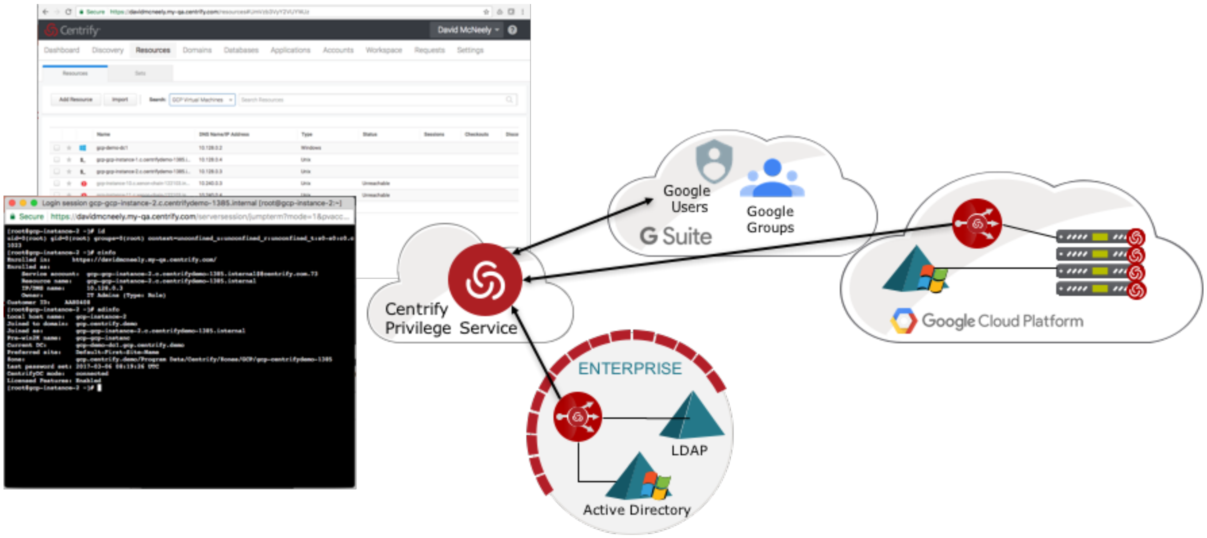
The Centrify Privileged Identity Management solution provides a set of controls for Google Compute Engine Linux VM Instances to support Enterprise integrated identity and access management functions. This solution enables organizations to consolidate identities, enforce cross-platform least privilege access and control shared accounts, while securing remote access and auditing all privileged sessions.

This guide will show how to setup and configure Active Directory based identity and access controls as well as privilege management for Linux VM Instances running on Google Cloud Platform. It will also show how to take over password management for local root accounts as well as to provide secure remote access to these Linux VM Instances.

Architecture

The Centrify PIM Solution is made of 2 components.

- Centrify Server Suite which is an agent based solution to provide Active Directory integration for user authentication, role-based access control and privilege elevation management for sudo equivalent capabilities. Many organizations choose to extend their Active Directory infrastructure to support identity and access management for systems and applications hosted within GCP.
- Centrify Privilege Service is built on the Centrify Identity Platform to provide shared account password management, application to application password management and secure remote access for Windows and Linux instances on GCP.



```
[root@gcp-instance-2 ~]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c
1023
[root@gcp-instance-2 ~]# cinfo
Enrolled in:      https://davidmcneely.my-qa.centrify.com/
Enrolled as:
    Service account:  gcp-gcp-instance-2.c.centrifydemo-1385.internal$@centrify.com.73
    Resource name:    gcp-gcp-instance-2.c.centrifydemo-1385.internal
    IP/DNS name:      10.128.0.3
    Owner:            IT Admins (Type: Role)
Customer ID:    AAB0408
[root@gcp-instance-2 ~]# adinfo
Local host name:   gcp-instance-2
Joined to domain:  gcp.centrify.demo
Joined as:         gcp-gcp-instance-2.c.centrifydemo-1385.internal
Pre-win2K name:    gcp-gcp-instanc
Current DC:        gcp-demo-dc1.gcp.centrify.demo
Preferred site:    Default-First-Site-Name
Zone:              gcp.centrify.demo/Program Data/Centrify/Zones/GCP/gcp-centrifydemo-1385
Last password set: 2017-03-06 08:19:36 UTC
CentrifyDC mode:   connected
Licensed Features: Enabled
[root@gcp-instance-2 ~]# 
```

The cost of the solution is based on the features and capabilities that you need, however you can get started using a Trial of the solution. Centrify offers both an Express version of Server Suite as well as a Trial (https://www.centrify.com/free-trial/) of both Server Suite and Privilege Service. This guide will use the Trial versions with full capabilities enabled.

You should also plan for the additional cost of Windows VM Instance(s) to run an Active Directory domain within your Project. While it is recommended to run at least 2 domain controllers in production, it is possible to get by with one domain controller for dev/test environments.

Deployment

There are several steps to this deployment which are mostly one time environment setup tasks. Once these steps are completed, you will be able to launch instances and have

Step 1: Setup Active Directory on GCP

First you will need to have an Active Directory Domain Controller setup operating as a "Resource Forest" within your GCP Project so that new VM Instances can join this AD domain.

- To setup an AD Domain Controller, following the instructions at: https://cloud.google.com/compute/docs/tutorials/setup-active-directory
- Note: you can run a dev or test environment with a single machine running a domain controller and perform all administrative work from the same computer, however in production you should plan for more than one domain controller for fault tolerance, lock down these systems and perform all administration from a separate Windows VM instance joined to the domain.

Optional: Site to Site VPN for 1-way trust. In most production use cases, you would setup the Domain running in your project as a Resource Forest with a 1-way trust to your existing on-premises Domain in order to grant existing user accounts from the on-premises Domain with rights to login to your new GCE Instances. In order to setup the 1-way trust, you will need to setup a site to site VPN in order to establish a 1-way trust with your on-premises Active Directory Domain. For Dev/Test environments, this is optional if you just want to create User accounts within the AD Domain vs. setup trust to leverage existing AD Accounts.

You should create an OU for the GCE Instances that you create for your Project.

- Login to the Domain Controller and launch Active Directory Users and Computers (ADUC), then create an Organizational Unit such as: OU = GCP-ProjectName

In order to automate the process for new virtual machines to join Active Directory, you will need to create an account that you delegate the appropriate rights to join computers to the OU you just created. This process is described in more detail in a HowTo article posted on the Centrify Community (http://community.centrify.com/t5/TechBlog/HOWTO-Use-Centrify-Tools-for-Public-Private-Cloud-Automation/ba-p/20369)

- Within ADUC, create a user account in the "Users" Container with a name such as "computerjoin@domain.com" with just a first name of "computerjoin".
    - Set the password to never expire and check the box to prevent the user from changing the password within the Account tab since this will be used as a service account.
- Grant this account delegated rights to join computers in the OU you just created.
    - Right click on the OU that you created earlier and select "Delegate Control…" then grant the adjoin user created above with following rights:
    - Select "Create a custom task to delegate"
    - Next select "Only the following objects in the folder" and select "Computer objects" and check the box for "Create selected objects in this folder" and "Delete selected objects in this folder".
    - Next check "Full Control" and Next to complete the delegation wizard.

You will also need to generate a Kerberos keytab file for this account. This keytab will hold a Kerberos credential which can later be used by the automation script to login to AD in order to perform the join operation for the new virtual machine

- Create the Keytab file for the "computerjoin" account that you just created.
    - On Windows use ktpass (reference https://technet.microsoft.com/en-us/library/cc753771.aspx)
        - Example: ktpass /princ computerjoin@YOURDOMAIN.COM /pass computerjoin-password /ptype KRB5_NT_PRINCIPAL /out computerjoin.keytab
    - On Linux with Centrify Server Suite agent use adkeytab (reference https://docs.centrify.com/en/css/suite2017/centrify-command-reference.pdf)
        - Example: adkeytab -A -K computerjoin.keytab -u your_admin -p your_admin_password computerjoin
- Upload this Keytab file (computerjoin.keytab) to a Google Storage Bucket which will be used later for joining the computer to AD.

Step 2: Setup Centrify Server Suite

You will need to install Centrify Server Suite management tools onto either a Windows VM Instance joined to your new domain to be used for administrative work or you can install these tools onto your Domain Controller. These tools enable you to create and manage policies stored in AD (using native object classes and schema) which will govern user access and their privileges across the VM Instances within your GCP environment.

Download and install Centrify Server Suite Standard Edition

- You can request a trial for Centrify Server Suite at https://www.centrify.com/free-trial/server-suite-form/
- Once you have requested a trial you will get Centrify Support Account setup so that you can login to Centrify Support Portal and access the Download Center.
- First you need to visit the Centrify Repo page in order to get your Repo Key, you will need this later for the scripts that automate the installation of Centrify for new virtual machines.
- Login to your Domain Controller that you setup in Step 1, then login to the Centrify Support portal and go to the Download Center in order to download Centrify Server Suite 2017 Standard Edition package as a Zip file.
    - **Note:** you may need to turn off Internet Explorer Safe Mode and add Centrify.com as a trusted site for downloading software.
- Expand the Zip file and launch the autorun program and then install Centrify DirectManage Access. You only need to select the defaults and continue with the installation.

Centrify Zones for Access and Privilege Management

- Launch the Centrify Access Manager from the icon on the desktop
- Create a Global Zone with the name of "GCP"

Delegate management to the "computerjoin" account to support auto-joining computers to the Zone "GCP"

- Right click on the GCP Zone and select "Delegate Zone Control…"
- Add your "computerjoin" account in the "Users, Groups, Computer or Service Accounts"
- Next delegate the tasks "Join computers to the zone", "Remove computers from the zone" and "Modify computer profiles"

- Click Next and Finish

Setup AD User Authorizations and Privileges to login to Linux Virtual Machines

- Within the Access Manager, open the GCP Global Zone
- Open UNIX Data and add your AD user account as a User so that you can define the UNIX attributes.
- Open Authorizations and right click on “Role Assignments” and select “Assign Role” to create a new role assignment
  - Select the “UNIX Login” Role
  - Add your own AD account in the Add User dialog.
  - You can always come back and define your own Roles with specific PAM Access and Command Rights

Step 3: Setup Centrify Privilege Service

Login to your Centrify Privilege Service (CPS) tenant via the account information that you should have received via email after your trial request.

- First, Change the initial Admin account’s password and add a mobile phone and valid email address so that you can turn on MFA.
- Next, Read the Getting Started Guide (https://docs.centrify.com/en/cps/centrify-cps-quickstart.pdf)

Optional: Setup a Connector for AD On-Premises AD user login. If you want to enable login with your existing Active Directory user accounts, then you need to install the

- Login to CPS and switch to the “Admin Portal” by clicking on your name.
- On the “Settings” tab, click on “Network” and “Centrify Connector”. From here click on “Add Centrify Connector” button in order to download, install and register the Connector.

Setup a Connector within the Project – In order to both enable the CPS to manage local shared accounts and to support secured remote access via CPS to virtual machines within the project, you will need to install a Centrify Connector on a Windows VM.

- Perform the same steps as above to install a Centrify Connector within the Project on a Windows VM.

Get an Enrollment Code and verify the Security Settings

- Click on your name and “Switch to Privilege Manager”
- Go to the “Settings” tab, then click on “Enrollment Codes”
  - Click “Add” to create an Enrollment Code
  - Add the System Administrator Role as the Owner. Note: you can always create another Role for this purpose and assign the members by name or by Group from your AD.
  - Adjust other parameters as desired and click on Save
- Verify the settings within “Account Permissions”, “Resource Permissions” and “Security Settings” are defined appropriately.

Step 4: Setup the GCP Environment for AD auto-join

Google will automatically setup your first project with the defaults which will work for this scenario. You will need to use your Active Directory Domain Controller for DNS, but the only required change is to the new Linux VM instances which will be handled by the startup script.

It is important to understand the concepts behind the startup scripts which Google has documented here: https://cloud.google.com/compute/docs/startupscript. Centrify has published a sample startup script that will automate the installation of Centrify agent, configuration and join to Active Directory as well as enrollment to Centrify Privilege Service. Once the script has finished, you will find the computer has an account in Active Directory and will show up in the CPS Portal where the root account will be vaulted for the virtual machine.

Create a Storage Bucket for storing the Startup Script and the computerjoin.keytab file created previously.

- Download and update the script located at https://github.com/centrify/GCP-Automation
- Once you have updated the user configuration data throughout the script, upload the file to the storage bucket that you created.

Verification of Normal Usage

This section will show you how to create new Linux VM instances where each instance will be auto-joined to AD and auto-enrolled for CPS management and secure remote access.

Step 1: Launch new VM Instances

- Login to your GCP Console at https://console.cloud.google.com
- Launch an instance and use the script to auto-join to AD
  - Give it a unique name as suggested, ex. “instance-1”
  - Select the appropriate Linux OS such as Red Hat or CentOS
  - Specify the Network Zone where your AD Domain Controller is located
  - Open the “Management, disk, networking, SSH keys” settings
    - Under Metadata
      - Specify a Key of “startup-script-url”
      - Specify a Value containing the URL for Storage Bucket such as “gs://your-bucketname/scriptname.sh” or “https://storage.cloud.google.com/your-bucketname/gcp_startup_CPS-AD.sh”
  - click Create
  - Once the machine has been created, it will launch the startup-script and enroll into CPS and join AD.

Step 2: Verify Proper Operation

Once the computer has finished launching and executing the startup script, you should be able to refresh the displays for both Active Directory Users and Computers (ADUC) and Centrify Privilege Service on the Resources tab to see the computer with the name that you gave it

- Verify the computer exist in both Active Directory and Centrify Privilege Service
- You should now be able to click on the computer in the CPS Portal and using the Account Actions task, login using the root account, or use manual login to use your Active Directory account for login.

Performance

Since the solution is a management platform for user authentication and privilege management, each agent that is installed on the Virtual Machines will perform the local enforcement of centralized policies stored within the Active Directory Domain. These policies are replicated across a Domain providing a highly available and fault tolerant solution once you deploy more than one domain controller within your project.

Centrify Privilege Service can also scale out to support additional Connectors for each project where the service will load balance across the available Connectors for each project or subnet.

Security

Security options you have for Shared Account Password Management features:

- Centrify operates the Privilege Service as a managed offering where all data is encrypted uniquely for each tenant and you have the option of using a SafeNet KeySecure for password storage if you need a higher level of security.
- Centrify also offers customers the ability to purchase the solution as software which you can install and run on your own Windows 2012r2 server where you maintain all controls over the encrypted data within the internal database.

Security considerations for user authentication:

- There are several options for managing Active Directory user authentication to GCP hosted virtual machines as outlined in this Centrify Blog article, http://blog.centrify.com/active-directory-active-hybrid-it/ .
- You should also consider turning on one of several Multi-Factor Authentication mechanisms that are built into the Centrify solution for ensuring authorized access by the right person at every authentication point within the solution.
    - Learn more about Centrify MFA Solutions: https://www.centrify.com/solutions/why-multi-factor-authentication/
    - Read HowTo articles on MFA: http://community.centrify.com/t5/TechBlog/bg-p/techblog/label-name/mfa

Operations

Centrify provides full audit logging across our products designed to rapidly assist administrators with any challenges they may face.

- Centrify Server Suite agent will log all message to syslog in both /var/log/messages and /var/log/secure log files. You should install the Google Logging Agent so that you can monitor events via the Stackdriver Logging console. Learn more here: https://cloud.google.com/logging/docs/agent/installation
- Centrify Privilege Service logs all activity and provides access to the events through both Dashboards and Reports within the Privilege Service portal.

Troubleshooting can be found in the Centrify Administrator's Guides each of our products as well as Server Suite's Planning and Config Guide.

- https://www.centrify.com/support/documentation/

Additional Resources

Learn more about the Centrify solution for Securing Hybrid Cloud at:

- https://www.centrify.com/solutions/secure-hybrid-cloud/

Visit the Centrify Community where you will find the TechCenter and TechBlogs for additional guidance, tips and tricks or join the discussion and ask questions.

- http://community.centrify.com/