November 2021

Binding Certificates to Service Accounts Deployed on Zero-Trust Cloud Virtual Machines

Assaf Namer

Binding Certificates to Service Accounts Deployed on Zero-Trust Cloud Virtual Machines

ABSTRACT

Zero-trust architecture is based on the assumption that none of the entities within the architecture are trusted implicitly based on their properties; explicit authentication and authorization based on certificates take place prior to establishing a session with the resource. However, there is no mechanism to monitor and enforce the distribution of certificates based on cloud-based service accounts. This disclosure describes techniques to bind a certificate policy to a service account that enables enforcement of specific policies on a virtual machine based on the particular service account associated with that virtual machine. The mapping between a certificate policy and the corresponding service account in the installed certificate is used to validate compliance with the policy. A mismatch between the policy in the presented certificate and the expected policy triggers an event that signals a potentially compromised virtual machine.

KEYWORDS

- Zero-trust architecture
- Zero-trust model
- Virtual Private Cloud (VPC)
- Virtual Machine (VM)
- Certificate Authority (CA)
- Certificate policy
- Transport Layer Security (TLS)
- mTLS
- Service account

BACKGROUND

Zero-trust architecture is commonly used for secure deployment of computing resources, whether in the cloud or in other computing infrastructure. Deployment of resources in a zero-trust architecture requires appropriate configuration of endpoints, applications, networks, infrastructure, and data. Such configuration is based on the assumption that none of the entities within the architecture are trusted implicitly based on one or more of their properties, such as location, network, ownership, etc. Instead, explicit authentication and authorization take place prior to establishing a session with the resource.

In the context of Virtual Privacy Cloud (VPC) networks, mutual Transport Layer Security (mTLS) and Secure Sockets Layer (SSL) inspection are methods that can be used effectively to maintain encryption while ensuring that the network is protected under the zero-trust model mentioned above. For instance, mTLS sessions are established based on certificates installed on virtual machines or any other compute services, such as containers. These certificates identify the machine on which they are installed, thus helping ensure the security of the established TLS connection. Currently, network administrators can issue certificates that specify particular policies, such as “the organization must be X.”

In addition to virtual machines, network identities can be used to create a virtual network segmentation in which machines that use the same service account can communicate with each other. A service account is an identity based on a virtual machine that exists only in the cloud environment. It represents policies and permissions assigned to the virtual machine. However, there is no mechanism to monitor and enforce the distribution of certificates based on service accounts.

DESCRIPTION

This disclosure describes techniques to bind a certificate policy to a service account in order to enable network administrators to enforce specific policies on a virtual machine based on the particular service account associated with that virtual machine. The mapping between a certificate policy and the corresponding service account in the installed certificate is used to validate compliance with the policy as presented to the Certificate Authority (CA) service.

The CA can employ various mechanisms to validate the integrity of the deployed certificates. For example, such mechanisms can include: periodically probing each virtual machine in the designated network to present a certificate; deploying virtual machines to perform packet mirroring such that each certificate presented by the virtual machine is mirrored to the CA for inspection; etc.

The CA compares the policy in the presented certificate against that on the record for the corresponding service account. A mismatch between the policy in the presented certificate and the expected policy results in the triggering of an event that signals a potentially compromised virtual machine. The triggered event can be used to take appropriate automated or manual action in response to the potential compromise.

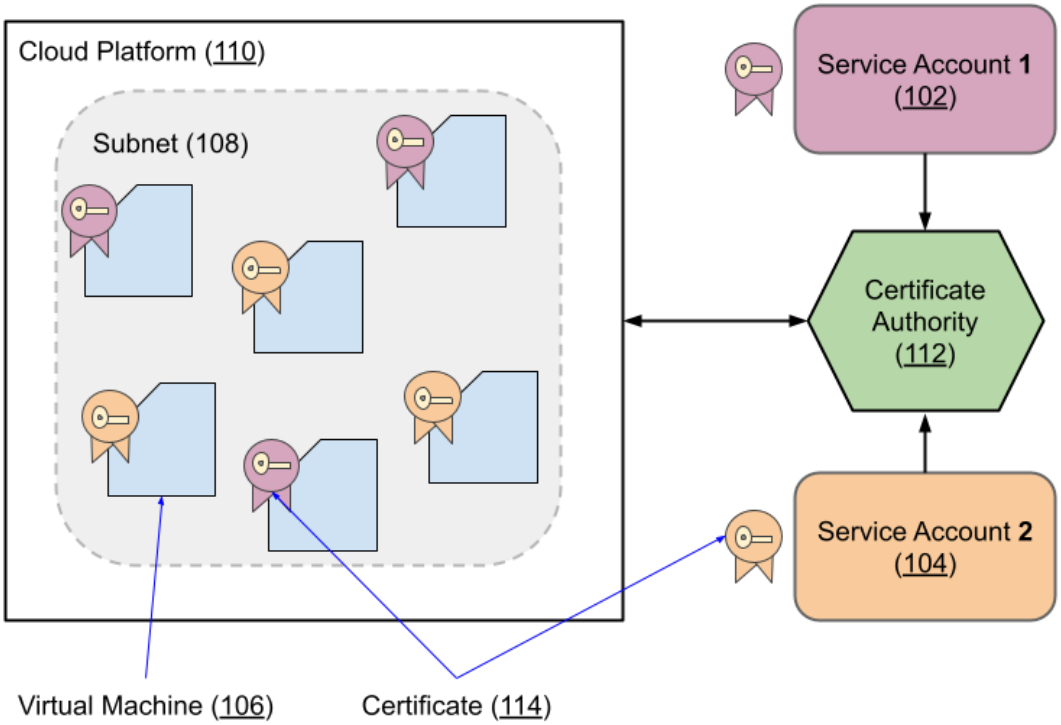

Fig. 1: Binding certificates to service accounts connected to virtual machines in the cloud

Fig. 1 shows an example of operational implementation of the techniques described in this disclosure. Two types of service accounts, Service Account 1 (102) and Service Account 2 (104) are provided with virtual machines (106) within a subnet (108) of a cloud platform (110). A private certificate authority for the cloud (112) is employed to generate certificates (114) such that specific certification parameters, such as name, lifetime, domain name, etc. are limited to the specific service account connected to the virtual machine on which the certificate is deployed. For example, Fig. 1 shows the certificate for Service Account 1 in purple and the one for Service Account 2 in orange.

Network administrators can use this approach to create granular segmentation within a subnet based on certificate identities connected to service accounts. Even if an adversary succeeds in compromising a virtual machine to obtain escalated privileges and modify the

certificate installed on the compromised virtual machine, the attack does not succeed because the modified certificate causes a mismatch thus revealing the (potentially) compromised status of the virtual machine.

Techniques described in this disclosure provide built-in enforcement mechanisms to ensure the integrity of certificates deployed on virtual machines. The centralized cloud-based approach can be employed to verify certificates and enforce policies at scale across multiple projects and subnets. Such ability to handle scale is particularly important for zero-trust architectures in which each machine and service account must authenticate prior to establishing a session and exchanging data. The techniques described in this disclosure can be used by any platform or service that provides cloud-based virtual machines and service accounts.

CONCLUSION

This disclosure describes techniques to bind a certificate policy to a service account that enables enforcement of specific policies on a virtual machine based on the particular service account associated with that virtual machine. The mapping between a certificate policy and the corresponding service account in the installed certificate is used to validate compliance with the policy. A mismatch between the policy in the presented certificate and the expected policy triggers an event that signals a potentially compromised virtual machine.