Locking it Down

You've done a lot of work so far to make sure your security and monitoring were in place, but there is still work to do to improve the security of your cluster.

Challenge

Your CTO is feeling confident in what your team has been able to accomplish, but there are still some security concerns you will need to address. After all, when dealing with sensitive information, security is one of the top concerns. As part of an effort to limit secrets stored in the cluster and to remove reliance on username and password authentication, the Trip service has been updated to enable SQL access via managed identity. Utilize this by setting up pod identity in your cluster.

In this challenge you must work to increase the security of your cluster by meeting these requirements:

1. Services in your cluster should only be able to make requests to other services if explicitly required.
2. None of the deployed services should be able to communicate with the api server.
3. None of the applications should run as root. This should be enforced by default.
4. Limit the egress traffic to only what is necessary.
5. Limit secrets stored in the cluster by implementing a managed identity for your services.

Success Criteria

- **Your team** restricted access from the deployed services access to kube-apiserver
- **Your team** limited the access to the Kubernetes API Server to only machines from your location
- **Your team** demonstrated that the API applications cannot call each other
- **Your team** restricted ability to deploy applications that have root access
- **Your team** limited the egress traffic from the cluster
- **Your team** enabled sql server access from inside the vnet only
- **Your team** has enabled the trip service access to SQL DB utilizing a managed identity.

References

Kubernetes

- Kubernetes Service Accounts (https://kubernetes.io/docs/reference/access-authn-authz/service-accounts-admin/)

AKS

- Azure Policy for Kubernetes clusters (https://docs.microsoft.com/en-us/azure/governance/policy/concepts/policy-for-kubernetes)
- Using Network Policies (https://docs.microsoft.com/en-us/azure/aks/use-network-policies)
- Secure access to the API server using authorized IP address ranges in AKS (https://docs.microsoft.com/en-us/azure/aks/api-server-authorized-ip-ranges)
- Control egress traffic for cluster nodes in AKS (https://docs.microsoft.com/en-us/azure/aks/limit-egress-traffic)
- Pod Identity (https://docs.microsoft.com/en-us/azure/aks/use-azure-ad-pod-identity)

Azure SQL Database

- Use virtual network service endpoints and rules for database servers (https://docs.microsoft.com/en-us/azure/sql-database/sql-database-vnet-service-endpoint-rule-overview)
- Azure CLI: az network vnet subnet update (https://docs.microsoft.com/en-us/cli/azure/network/vnet/subnet?view=azure-cli-latest#az-network-vnet-

- Managed Identities in SQL (https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/tutorial-windows-vm-access-sql)