Microsoft Azure Red Hat OpenShift security FAQ

SRE access

Question: How do site reliability engineers (SREs) access my Microsoft Azure Red Hat® OpenShift® cluster? Does it go through the public internet?

Answer: SREs access the cluster through Azure Private Link, which maps private points to Azure resources.

See the cluster configuration requirements section.

Question: What permissions do I need to run an Azure Red Hat OpenShift cluster?

Answer: To deploy and run an Azure Red Hat OpenShift cluster, you will need to create a service principal. You can create a service principal by using the Azure command-line interface (CLI) or PowerShell. In this case, you will need sufficient permissions to create the application on Azure Active Directory—either a member user of the tenant or a guest user that has been assigned the application administrator role.

If a service principal already exists and is provided for the deployment of the Azure Red Hat OpenShift cluster, you do not need the aforementioned permissions on Azure Active Directory.

In both cases, the service principal needs the roles contributor and user access administrator.

Question: What is the identity and access management (IAM) policy for either of the above?

Answer: The service principal needs to have the roles contributor and user access administrator.

See link.

Question: What level of access do SREs have to my Azure Red Hat OpenShift cluster? Can they access my applications and data?

Answer: No, the SREs can only access the Azure Red Hat OpenShift at platform level (control plane nodes). They use the connection through an Azure Private Link that allows communication to an internal load balancer behind the control plane nodes. The worker nodes—where applications run—are behind a different load balancer, which SREs do not have access to.

Question: If an SRE needs access to my cluster, what is the process for gaining access and how is auditing handled?

Answer: Audit logs are generated and kept and customers can request them.

SRE personnel objections

Question: Where are SREs located?

Answer: There is no list of locations for SREs.

Question: Our company has a policy on not using services from a particular country, can we exclude a country from having SREs work on our cluster?

Answer: This is not possible as of now.

Customer process and tooling

Question: InfoSec requires us to install a traditional security tool on all servers. Can I install these on the Azure Red Hat OpenShift hosts?

Answer: Azure Red Hat OpenShift hosts run CoreOS, which is an OS with the bare minimum and is not intended to have anything that does not come out of the box installed on it.

Question: Can we get access to the SRE logging system and forward to our centralized logging solution?

Answer: For cluster operations and audit, the customer cluster administrators can deploy an optional logging stack to aggregate all logs from their Azure Red Hat OpenShift cluster. For example, administrators can aggregate node system audit logs and infrastructure logs. However, these logs consume other cluster resources.

The virtual machine (VM) logs where the nodes run are not exposed to customers.

Question: What steps are taken to harden the Azure Red Hat OpenShift cluster?

Answer: Using Azure Front Door, Azure Private Link, the internal load balancers, and Azure Firewall—as shown in the portfolio architecture—ensures the protection of the Azure Red Hat OpenShift cluster.

About Red Hat

Red Hat is the world's leading provider of enterprise open source software solutions, using a community-powered approach to deliver reliable and high-performing Linux, hybrid cloud, container, and Kubernetes technologies. Red Hat helps customers develop cloud-native applications, integrate existing and new IT applications, and automate and manage complex environments. A trusted adviser to the Fortune 500, Red Hat provides award-winning support, training, and consulting services that bring the benefits of open innovation to any industry. Red Hat is a connective hub in a global network of enterprises, partners, and communities, helping organizations grow, transform, and prepare for the digital future.

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

redhat.com
#287611_0423