Red Hat OpenShift Service on AWS security FAQ

Questions are valid for Red Hat OpenShift 4

SRE access

Question: How do site reliability engineers (SREs) access my Red Hat® OpenShift® Service on AWS cluster by default?

Answer: SRE access to Red Hat OpenShift Service on AWS clusters is controlled through several layers of required authentication, all of which are managed by strict company policy. All authentication attempts to access a cluster, in addition to changes made within a cluster, are recorded within audit logs, along with the specific account identity of the SRE responsible for those actions. These audit logs help ensure that all changes made by SREs to a customer's cluster adhere to the strict policies and procedures that make up Red Hat's managed services guidelines.

The information presented below is an overview of the process an SRE must perform to access a customer's cluster.

- The SRE makes a request to refresh the ID token from Red Hat's single sign-on (SSO) technology (Red Hat Cloud Services).
- The SRE sends a request tunneled through the Red Hat virtual private network (VPN). This request is made via the corporate identity and access management (IAM) system; authentication is multifactor (made up of a password and an ephemeral one-time token). Once the SRE authenticates and is allowed access to the orchestration and management systems, the authorization is managed by Red Hat corporate directory services. The use of IAM allows SREs to be managed internally per organization via groups and existing on-boarding/off-boarding processes. Changes to the orchestration and management systems require many layers of approval and are maintained by strict company policy.
- Once authorized, the SRE logs into the fleet management plane and receives a service account token that the fleet management plane created. The token is valid for 12 minutes. Once the token is no longer valid, it is deleted.
- With access granted to the fleet management plane, the SRE uses various methods to access clusters, depending on network configuration.
  - Accessing a private or public cluster: A request is sent through a specific Network Load Balancer (NLB) using an encrypted HTTP connection on port 6443. The NLB contains an IP allowlist so the application programming interfaces (APIs) accept connections from a specific set of IPs—of which the fleet management plane contains.
  - Accessing a PrivateLink cluster: A request is sent to the Red Hat Transit Gateway, which then connects to a Red Hat virtual private cloud (VPC) per region. The VPC that receives the request will be dependent on the target private cluster's region. Within the VPC, there is a private subnet, which contains the PrivateLink endpoint to the customer's PrivateLink cluster.

SREs access private clusters using an encrypted HTTP connection. Connections are permitted only from a security-safe Red Hat network using either an IP allowlist or a private cloud provider link.

Question: How does Amazon Web Service (AWS) PrivateLink change the way SREs access my OpenShift Service on AWS cluster?

Answer: When you have a PrivateLink OpenShift Service on AWS cluster, its Kubernetes API server is exposed through a load balancer that can only be accessed from within the VPC by default. Red Hat SREs can connect to this load balancer through a VPC endpoint service that has an associated VPC endpoint in a Red Hat-owned AWS account. This endpoint service contains the name of the cluster, which is also in the Amazon Resource Name (ARN).

Under the Allow principals tab, a Red Hat-owned AWS account is listed. This specific user ensures that other entities cannot create VPC endpoint connections to the PrivateLink cluster's Kubernetes API server.

When Red Hat SREs access the API, this fleet management plane can connect to the internal API through the VPC endpoint service.

Question: What permissions do I need to run an OpenShift Service on AWS cluster?

Answer: The recommended implementation is using the AWS Security Token Service (STS). After the cluster is created, an identity provider must be configured so that the accesses will be validated by it. This is a list of supported providers.

It is a best practice for the OpenShift Service on AWS cluster to be hosted in an AWS account within an AWS organizational unit (OU). A service control policy (SCP) is created and applied to the AWS OU that manages what services the AWS subaccounts are permitted to access. The SCP applies only to available permissions within a single AWS account for all AWS subaccounts within the OU. It is also possible to apply a SCP to a single AWS account. All other accounts in the customer's AWS organizations are managed in whatever manner the customer requires. Red Hat SREs will not have control over SCPs within AWS organizations.

In the case of customers who, despite the recommendation, have not yet chosen to build OpenShift Service on AWS clusters in STS mode, Red Hat must have the administrator access policy applied to the administrator role at all times.

To deploy an OpenShift Service on AWS cluster that uses the AWS Security Token Service (STS), customers must create the following AWS IAM resources:

- Specific account-wide IAM roles and policies that provide the STS permissions required for OpenShift Service on AWS support, installation, control plane, and compute functionality. This includes account-wide operator policies. These are provided by OpenShift Service on AWS command line interface (CLI).
- Cluster-specific operator IAM roles that permit the OpenShift Service on AWS cluster operators to carry out core OpenShift functionality. These are provided by the OpenShift Service on AWS CLI.
- An OpenID Connect (OIDC) provider that the cluster operators use to authenticate. Also provided by OpenShift Service on AWS CLI.
- If OpenShift Service on AWS is deployed by using Red Hat OpenShift Cluster Manager, these additional resources must be created:
  - An ocm-role to complete the installation on the cluster.

- A user role without any permissions to verify the AWS account identity.
- Both are provided by OpenShift Service on AWS CLI.

STS is the recommended credential mode because of the enhanced security it provides.

Question: What is the IAM policy for implementations with STS and for those without it?

Answer: This is the reference for IAM policies when using STS, which is the recommended implementation.

In the case that a customer is still not using STS, Red Hat must have the administrator access policy applied to the administrator role at all times. Red Hat is responsible for creating and managing IAM policies, IAM users, and IAM roles. Review a description of the administratoraccess policy.

When you install an OpenShift Service on AWS cluster that uses the AWS Security Token Service (STS), cluster-specific Operator AWS Identity and Access Management (IAM) roles are created. These IAM roles permit the OpenShift Service on AWS cluster Operators to run core OpenShift functionality.

Cluster Operators use service accounts to assume IAM roles. When a service account assumes an IAM role, temporary STS credentials are provided for the service account to use in the cluster Operator's pod. If the assumed role has the necessary AWS privileges, the service account can run AWS software development kit (SDK) operations in the pod.

Question: What level of access do SREs have to my OpenShift Service on AWS cluster? Can they access my applications and data?

Answer: An SRE adheres to the principle of least privilege when accessing OpenShift Service on AWS and AWS components. There are 4 basic categories of manual SRE access:

- SRE access through the Red Hat Portal with normal two-factor authentication and no privileged elevation.
- SRE access through the Red Hat corporate SSO with normal two-factor authentication and no privileged elevation.
- Red Hat OpenShift elevation, which is a manual elevation using Red Hat SSO. Access is audited.
- AWS access or elevation, which is a manual elevation for AWS console or CLI access. Access is limited to 60 minutes and is fully audited.

Question: Are there SRE audit logs for what was done or accessed? How do we get access to these?

Answer: SREs must authenticate as individuals to ensure auditability. All authentication attempts are logged to a Security Information and Event Management (SIEM) system.

SRE personnel objections

Question: Where are the SREs located?

Answer: Review the Red Hat subprocessor list.

Customer process and tooling

Question: InfoSec requires us to install a traditional security tool on all servers. Can I install these on OpenShift Service on AWS hosts?

Answer: This is not supported. See policies and service definitions for details.

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

Answer: OpenShift Service on AWS provides optional integrated log forwarding to Amazon CloudWatch.

Question: What steps are taken to harden the OpenShift Service on AWS cluster?

Answer: Apart from the use of load balancers and PrivateLink, each OpenShift Service on AWS cluster is protected by a security-focused network configuration using firewall rules for AWS security groups. OpenShift Service on AWS customers are also protected against distributed denial-of-service (DDoS) attacks with AWS Shield Standard.

Red Hat performs periodic penetration tests against OpenShift Service on AWS. Tests are performed by an independent internal team by using industry standard tools and best practices. Any issues that may be discovered are prioritized based on severity. Any issues found belonging to open source projects are shared with the community for resolution.

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
#550750_1023