Automate network management with Red Hat and F5

Businesses are looking for ways to improve modern and legacy applications using DevOps to eliminate bottlenecks and automation to speed up workflows. These applications need traditional delivery services like identity and access management, web application security, and TCP optimization to make sure they maintain performance and security. In addition, the open nature of the internet exposes organizations to cyber attacks from any location, and the scale and complexity of these attacks can put any system at risk.

Red Hat and F5 have partnered to automate, scale, and protect application workloads across hybrid cloud environments. Together, Red Hat and F5 provide protection at both the application and network levels.

Automate installation and deployment tasks

Installing and maintaining applications on each physical or virtual device across one or many networks can be difficult, especially with all the intricacies a hybrid cloud environment can bring. Red Hat® Ansible® Automation Platform works with F5 to give you an automated installation and deployment environment that simplifies installing applications on every device, reducing the number of IT resources required and improving reliability, efficiency, and agility.

You do not have to install any new software to get started. If you are already working with F5, you can automate operations using Ansible Automation Platform through a series of integrations with the F5 BIG-IP modules. You can create F5 deployment and configuration templates once in an Ansible Automation Platform playbook, then use them across your entire organization.

Advanced application services can also be added to your container deployments, using F5 Container Ingress Services (CIS). This includes ingress control HyperText Transfer Protocol (HTTP) routing, load balancing, and application delivery performance, as well as robust security-oriented services. You can also use Red Hat OpenShift® to provide a single window to monitor transactions and safety alerts. Red Hat OpenShift allows you to validate new programming before making changes, making the process of updating your infrastructure safer. You can also make these changes without advanced scheduling or maintenance windows.

The ability to see how applications react in your applications also gives you the ability to look forward. You can analyze sophisticated real-time data to adapt to changing conditions across platforms, defend against evolving threats, and deliver the digital experiences your customers demand.

Scale your network environment efficiently

With Red Hat OpenShift, you can integrate F5 BIG-IP devices using CIS and deploy application services in less time and with less effort across local and cloud environments. Red Hat OpenShift makes it easier to create, test, and apply applications in your hybrid or multicloud environment. Applications can be run and tested before they are released and then be added automatically to your hybrid or multicloud environment.

Using Red Hat OpenShift, combined with F5 CIS, services can be defined once, then applied across your entire network. Developers can create applications without worrying about the structure of the Kubernetes packages, allowing for scalability across cloud platforms.

Protect your network against outside attacks

Ansible Automation Platform and F5 can help you reduce security issues, from errors that occur when applications do not work together correctly to outside attacks that threaten a single node or your entire system. You can use Red Hat OpenShift to monitor all system interactions through the management window, reducing the time an outside application has access to your system.

Using F5 and Ansible Automation Platform together gives you the ability to add trustworthy security checks throughout your system, watching for problems that may appear anywhere within it. F5 offers protection against emerging threats, bot detection, API security, and distributed denial of services (DDOS) attacks. Ansible Automation Platform can add protection with network firewalls, an intrusion detection system (IDS), and a security information and detection system (SIEM).

Monitoring your entire system through a single window gives you the ability to catch problems as they occur. You can then use preapproved automation workflows to route calls from other departments, analyze and test the problem, and to correct the problem by ignoring it, isolating the traffic, or correcting the problem while notifying no other departments.

You can monitor Kubernetes objects with Red Hat OpenShift. Advanced web application firewall (AWAF) protection, and authentication are provisioned with different Kubernetes objects and comply with Kubernetes role-based access control (RBAC) practices. If BIG-IP Advance WAF or NGINX App Protect detects suspicious traffic, an alert with details is sent to the Elasticsearch, Logstash, and Kibana (ELK) stack, which indexes and processes the data, and then executes a predefined Ansible Playbook to enforce security policy. Both Advanced WAF and NGINX App Protect continually export detailed data into Elasticsearch, helping you monitor all of your network and apps. This approach provides a balance between the speed of new features and the reliability your users depend on.

Conclusion

As environments become more hybrid, the need for automated and security-focused infrastructure increases. F5 and Red Hat give you the tools you need to automate tasks across networks, scale installations and deployments to the size you need for your business, and protect your infrastructure against attack.

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

f facebook.com/redhatinc
🐦 @RedHat
in 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
#F31395_0422