What's New with SUSE CaaS Platform?

SUSE CaaS Platform continues to deliver rapid advancements, with expanded options for cluster optimization, support for more efficient and secure container image management, simplified ingress control and an updated release of Kubernetes for enhanced security.

With SUSE CaaS Platform you can:

1 **Optimize your cluster configuration** with expanded data center integration and cluster re-configuration options.

Setting up your Kubernetes environment is easier than ever with improved integration of private (OpenStack) and public (Amazon Web Services, Microsoft Azure and Google Cloud Platform) cloud storage and automatic deployment of the Kubernetes software load balancer.

A new SUSE toolchain module also allows you to tune the MicroOS container operating system to support your custom hardware configuration needs. Now you can, for example, install additional packages required to run your own monitoring agent or other custom software.

Transform your start-up cluster into a highly available environment. With new cluster reconfiguration capabilities, you can switch from a single-master to a multi-master environment, or vice-versa, to accommodate your changing needs.

With LDAP and OIDC integration, you can configure SUSE CaaS Platform to use your existing enterprise directory to verify user credentials. This eliminates the need to set up and maintain SUSE CaaS Platform—specific user and group information, saving time while simplifying credential maintenance for users.

2 **Manage container images more efficiently and securely** with a local container registry.

Download a container image from an external registry once, and then save a copy in your own local registry for sharing among all nodes in your cluster. By connecting to an internal proxy rather than an external registry and by downloading from a local cache rather than a remote server, you will improve security and increase performance every time a cluster node pulls an image from the local registry.

For even greater security, disconnect from external registries altogether and use only trusted images that you have loaded into your local registry.

Try out the new, lightweight CRI-O container runtime, designed specifically for Kubernetes and now supported in SUSE CaaS Platform. Stable and secure, CRI-O is also smaller and architecturally simpler than traditional container runtimes.

3 **Simplify management of external connectivity to Kubernetes managed services** with ingress controller support.

Reduce complexity through centralized management of IP addresses, TLS termination, customized URLs and internal load balancing.

4 **Harness Kubernetes advancements** in an enterprise ready platform.

SUSE CaaS Platform supports stable features in upstream Kubernetes code to bring you the innovation of Kubernetes in a platform that is easier for enterprises to consume and manage.

SUSE CaaS Platform is currently based on Kubernetes 1.10, which introduced a critical fix for the severe Privilege Escalation Vulnerability. This fix ensures unauthenticated users cannot perform privilege escalation and gain full admin privileges on a cluster.

Feel free to reach out to SUSE directly if you have any questions about a particular feature.
suse.com/caas