Red Hat
Advanced Cluster Security
for Kubernetes

ocp4-stig-v2r1 Compliance Report

Sep 03, 2025

Cluster	Control	Compliance
api-server-encryption-provider-cipher - Configure the Encryption Provider Cipher (CIS-OCP 1.2.31;2.8)	api-server-encryption-provider-cipher	100%
api-server-tls-security-profile - Ensure APIServer is configured with secure tlsSecurityProfile	api-server-tls-security-profile	100%
audit-error-alert-exists - Ensure that Audit Log Errors Emit Alerts	audit-error-alert-exists	100%
audit-log-forwarding-enabled - Ensure that Audit Log Forwarding Is Enabled (CIS-OCP 1.2.21)	audit-log-forwarding-enabled	0%
audit-log-forwarding-uses-tls - Ensure that Audit Log Forwarding Uses TLS	audit-log-forwarding-uses-tls	0%
audit-profile-set - Ensure that the cluster's audit profile is properly set (CIS-OCP 3.2.2)	audit-profile-set	100%
classification-banner - Enable Classification Banner on OpenShift Console	classification-banner	0%
cluster-logging-operator-exist - Ensure that OpenShift Logging Operator is scanning the cluster	cluster-logging-operator-exist	0%
cluster-version-operator-exists - Ensure that Cluster Version Operator is deployed	cluster-version-operator-exists	100%
cluster-version-operator-verify-integrity - Ensure that Cluster Version Operator verifies integrity	cluster-version-operator-verify-integrity	100%
configure-network-policies - Ensure that the CNI in use supports Network Policies (CIS-OCP 5.3.1)	configure-network-policies	100%
configure-network-policies-namespaces - Ensure that application Namespaces have Network Policies defined. (CIS-OCP 5.3.2)	configure-network-policies-namespaces	100%
container-security-operator-exists - Make sure the Container Security Operator is installed	container-security-operator-exists	0%
fips-mode-enabled-on-all-nodes - Ensure that FIPS mode is enabled on all cluster nodes	fips-mode-enabled-on-all-nodes	0%
idp-is-configured - Configure An Identity Provider (CIS-OCP 3.1.1)	idp-is-configured	0%
image-pruner-active - Configure ImagePruner so that images that are no longer needed are automatically removed	image-pruner-active	100%
imagestream-sets-schedule - All configured ImageStreams are configured to periodically check for updates	imagestream-sets-schedule	0%
ingress-controller-tls-security-profile - Ensure IngressController is configured to use secure tlsSecurityProfile	ingress-controller-tls-security-profile	100%
kubeadmin-removed - Ensure that the kubeadmin secret has been removed (CIS-OCP 3.1.1;5.1.1)	kubeadmin-removed	0%
oauth-login-template-set - Ensure that the OpenShift OAuth login template is set	oauth-login-template-set	100%
oauth-logout-url-set - Ensure that the OpenShift OAuth logout URL is set	oauth-logout-url-set	0%
oauth-or-oauthclient-inactivity-timeout - Configure OAuth tokens to expire after a set period of inactivity	oauth-or-oauthclient-inactivity-timeout	100%
oauth-or-oauthclient-token-maxage - Configure OAuth tokens to expire after a set period of inactivity	oauth-or-oauthclient-token-maxage	100%
oauth-provider-selection-set - Ensure that the OpenShift OAuth provider selection is set	oauth-provider-selection-set	0%
ocp-allowed-registries - Allowed registries are configured (CIS-OCP 5.5.1)	ocp-allowed-registries	0%
ocp-allowed-registries-for-import - Allowed registries for import are configured (CIS-OCP 5.5.1)	ocp-allowed-registries-for-import	0%
ocp-idp-no-htpasswd - Do Not Use htpasswd-based IdP	ocp-idp-no-htpasswd	100%
ocp-insecure-allowed-registries-for-import - Check configured allowed registries for import uses secure protocol (CIS-OCP 5.5.1)	ocp-insecure-allowed-registries-for-import	100%
ocp-insecure-registries - Check if any insecure registry sources is configured (CIS-OCP 5.5.1)	ocp-insecure-registries	100%
ocp-no-ldap-insecure - Only Use LDAP-based IdPs with TLS	ocp-no-ldap-insecure	100%
openshift-motd-exists - Ensure that the OpenShift MOTD is set	openshift-motd-exists	0%
project-config-and-template-network-policy - Ensure that project templates autocreate Network Policies	project-config-and-template-network-policy	100%
project-config-and-template-resource-quota - Ensure that project templates autocreate Resource Quotas	project-config-and-template-resource-quota	100%
rbac-least-privilege - Ensure that the RBAC setup follows the principle of least	rbac-least-privilege	N/A

privilege (CIS-OCP 5.2.10)		
rbac-logging-del - Ensure that the ClusterLogging and ClusterLoggingForwarder resources are protected from unauthorized deletion	rbac-logging-del	N/A
rbac-logging-mod - Ensure that the ClusterLogging and ClusterLoggingForwarder resources are protected from unauthorized modification	rbac-logging-mod	N/A
rbac-logging-view - Ensure that the ClusterLogging and ClusterLoggingForwarder resources are protected from unauthorized access	rbac-logging-view	N/A
resource-requests-quota-per-project - Ensure workloads use resource requests and limits per namespace	resource-requests-quota-per-project	100%
routes-rate-limit - Ensure that all Routes has rate limit enabled	routes-rate-limit	0%
scansettingbinding-exists - Ensure that Compliance Operator is scanning the cluster	scansettingbinding-exists	100%
scansettings-have-schedule - Ensure that Compliance Operator scans are running periodically	scansettings-have-schedule	100%
scc-limit-host-dir-volume-plugin - Limit Containers Ability to use the HostDir volume plugin (CIS-OCP 5.2.12)	scc-limit-host-dir-volume-plugin	N/A
scc-limit-host-ports - Limit Containers Ability to bind to privileged ports	scc-limit-host-ports	N/A
scc-limit-ipc-namespace - Limit Access to the Host IPC Namespace (CIS-OCP 5.2.3)	scc-limit-ipc-namespace	N/A
scc-limit-network-namespace - Limit Access to the Host Network Namespace (CIS-OCP 5.2.4)	scc-limit-network-namespace	N/A
scc-limit-privileged-containers - Limit Privileged Container Use (CIS-OCP 5.2.1)	scc-limit-privileged-containers	N/A
scc-limit-process-id-namespace - Limit Access to the Host Process ID Namespace (CIS-OCP 5.2.2)	scc-limit-process-id-namespace	N/A
scc-limit-root-containers - Limit Container Running As Root User (CIS-OCP 5.2.6)	scc-limit-root-containers	N/A
version-detect-in-hypershift - This is a helper rule to fetch the required api resource for detecting HyperShift OCP version	version-detect-in-hypershift	N/A
version-detect-in-ocp - This is a helper rule to fetch the required api resource for detecting OCP version	version-detect-in-ocp	N/A