Соответствие платформы стандартам безопасности

Данный раздел содержит справочную информацию по соответствию платформы стандартам безопасности.

1. CIS Kubernetes Benchmark

Центр интернет-безопасности - The Center for Internet Security (CIS) регулярно публикует документ, в котором содержится набор определенных шагов для обеспечения безопасности инфраструктуры Kubernetes. Данный раздел документации содержит сведения о соответствии платформы Nova Container Platform стандарту ***CIS Kubernetes Benchmark V1.9.0 - 03-25-2024***.

Скачать документ вы можете на официальном сайте CIS или получить копию по ссылке.

2. Компоненты Control Plane

2.1. Конфигурация узлов Control Plane

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
1.1.1	Ensure that the API server pod specification file permissions are set to 600 or more restrictive (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.1.2	Ensure that the API server pod specification file ownership is set to root:root (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.1.3	Ensure that the controller manager pod specification file permissions are set to 600 or more restrictive (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.1.4	Ensure that the controller manager pod specification file ownership is set to root:root (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform

1.1.5	Ensure that the scheduler pod specification file permissions are set to 600 or more restrictive (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.1.6	Ensure that the scheduler pod specification file ownership is set to root:root (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.1.7	Ensure that the etcd pod specification file permissions are set to 600 or more restrictive (Automated)	1 (Мастер-узлы)	✅ Соответствует	При автоматизированной проверке по данному шагу может быть получен результат *Fail*. Это связано с тем, что проверка выполняется по файлу `/etc/kubernetes/manifests/etcd.yaml`, который отсутствует в конфигурации Nova Container Platform. В платформе Etcd работает как служба Systemd, используя конфигурацию из файла `/etc/etcd.env`, права на который установлены в соответствие с рекомендацией.	Nova Container Platform
1.1.8	Ensure that the etcd pod specification file ownership is set to root:root (Automated)	1 (Мастер-узлы)	✅ Соответствует	При автоматизированной проверке по данному шагу может быть получен результат *Fail*. Это связано с тем, что проверка выполняется по файлу `/etc/kubernetes/manifests/etcd.yaml`, который отсутствует в конфигурации Nova Container Platform. В платформе Etcd работает как служба Systemd, используя конфигурацию из файла `/etc/etcd.env`, владельцем которого является пользователь `root:root`.	Nova Container Platform
1.1.9	Ensure that the Container Network Interface file permissions are set to 600 or more restrictive (Manual)	1 (Мастер-узлы)	✅ Соответствует	При автоматизированной проверке по данному шагу может быть получен результат *Warn*. Это связано с тем, что проверку нужно осуществлять по файлу конфигурации плагина, например /etc/kubernetes/cilium/cilium-config.yaml, права на который установлены в соответствие с рекомендацией	Nova Container Platform
1.1.10	Ensure that the Container Network Interface file ownership is set to root:root (Manual)	1 (Мастер-узлы)	✅ Соответствует	При автоматизированной проверке по данному шагу может быть получен результат *Warn*. Это связано с тем, что проверку нужно осуществлять по файлу конфигурации плагина, например /etc/kubernetes/cilium/cilium-config.yaml, владельцем которого является пользователь `root:root`	Nova Container Platform

1.1.11	Ensure that the etcd data directory permissions are set to 700 or more restrictive (Automated)	1 (Мастер-узлы)	✅ Соответствует	При автоматизированной проверке по данному шагу может быть получен результат *Fail*, поскольку сервис Etcd в Nova запускается с использованием переменных окружения в файле `/etc/etcd.env`. Поэтому в выводе команды `ps`, которую использует автоматическая проверка, отсутствуют какие-либо ключи, указывающие на параметр `DATA_DIR` etcd. Права на директорию `/var/lib/etcd` установлены согласно рекомендации.	Nova Container Platform
1.1.12	Ensure that the etcd data directory ownership is set to etcd:etcd (Automated)	1 (Мастер-узлы)	✅ Соответствует	При автоматизированной проверке по данному шагу может быть получен результат *Fail*, поскольку сервис Etcd в Nova запускается с использованием переменных окружения в файле `/etc/etcd.env`. Поэтому в выводе команды `ps`, которую использует автоматическая проверка, отсутствуют какие-либо ключи, указывающие на параметр `DATA_DIR` etcd. Автоматизированная проверка не может установить владельца директории, поскольку директория не может быть найдена. Владелец директории `/var/lib/etcd` согласно рекомендации.	Nova Container Platform
1.1.13	Ensure that the default administrative credential file permissions are set to 600 (Automated)	1 (Мастер-узлы)	✅ Соответствует	При автоматизированной проверке по данному шагу может быть получен результат *Fail*, т.к автоматический тест использует команду по проверке прав с ошибкой. Проверить права файла можно командой `stat -c %a /etc/kubernetes/admin.conf`.	Nova Container Platform
1.1.14	Ensure that the default administrative credential file ownership is set to root:root (Automated)	1 (Мастер-узлы)	✅ Соответствует	При автоматизированной проверке по данному шагу может быть получен результат *Fail*, т.к автоматический тест использует команду по проверке владельца файла с ошибкой. Проверить владельца файла можно командой `stat -c %U:%G /etc/kubernetes/admin.conf`.	Nova Container Platform
1.1.15	Ensure that the scheduler.conf file permissions are set to 600 or more restrictive (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.1.16	Ensure that the scheduler.conf file ownership is set to root:root (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform

1.1.17	Ensure that the controller-manager.conf file permissions are set to 600 or more restrictive (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.1.18	Ensure that the controller-manager.conf file ownership is set to root:root (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.1.19	Ensure that the Kubernetes PKI directory and file ownership is set to root:root (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.1.20	Ensure that the Kubernetes PKI certificate file permissions are set to 600 or more restrictive (Manual)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.1.21	Ensure that the Kubernetes PKI key file permissions are set to 600 (Manual)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform

2.2. Конфигурация сервера Kubernetes API

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
1.2.1	Ensure that the --anonymous-auth argument is set to false (Manual)	1 (Мастер-узлы)	⚠️ Внимание	В платформе используются методы авторизации RBAC, Node. Получить информацию о ресурсах Kubernetes без прохождения данных методов авторизации не предоставляется возможным. Анонимные запросы к Kubernetes API разрешены для проверочных healthcheck-запросов, которые выполняет компонент Kubelet.	Nova Container Platform
1.2.2	Ensure that the --token-auth-file parameter is not set (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.3	Ensure that the --DenyServiceExternalIPs is set (Manual)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform

1.2.4	Ensure that the --kubelet-client-certificate and --kubelet-client-key arguments are set as appropria (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.5	Ensure that the --kubelet-certificate-authority argument is set as appropriate (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.6	Ensure that the --authorization-mode argument is not set to AlwaysAllow (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.7	Ensure that the --authorization-mode argument includes Node (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.8	Ensure that the --authorization-mode argument includes RBAC (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.9	Ensure that the admission control plugin EventRateLimit is set (Manual)	1 (Мастер-узлы)	⚠️ Внимание	В платформе Nova по умолчанию данный плагин отключен, поскольку его параметры сильно зависят от возможной нагрузки на API-сервер Kubernetes. При небольшой нагрузке на API-сервер и высоком значении EventRateLimit, конфигурация будет неэффективна, и наоборот. Поэтому необходимо принимать решение о настройке параметра исходя из особенностей собственной инфраструктуры и запускаемых сервисов.	Пользователь Nova Container Platform
1.2.10	Ensure that the admission control plugin AlwaysAdmit is not set (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.11	Ensure that the admission control plugin AlwaysPullImages is set (Manual)	1 (Мастер-узлы)	⚠️ Внимание	В платформе Nova по умолчанию данный плагин отключен, так его включение влечет за собой увеличенную нагрузку на сетевую инфраструктуру и хранилище образов. При этом, кеширование образов на узлах кластера создает риск доступа к образу, зная его имя, без необходимой учетной записи. Данный параметр необходимо включать исходя из особенностей собственной инфраструктуры и запускаемых сервисов.	Пользователь Nova Container Platform

1.2.12	Ensure that the admission control plugin ServiceAccount is set (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.13	Ensure that the admission control plugin NamespaceLifecycle is set (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.14	Ensure that the admission control plugin NodeRestriction is set (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.15	Ensure that the --profiling argument is set to false (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.16	Ensure that the --audit-log-path argument is set (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.17	Ensure that the --audit-log-maxage argument is set to 30 or as appropriate (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.18	Ensure that the --audit-log-maxbackup argument is set to 10 or as appropriate (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.19	Ensure that the --audit-log-maxsize argument is set to 100 or as appropriate (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.20	Ensure that the --request-timeout argument is set as appropriate (Manual)	1 (Мастер-узлы)	⚠️ Внимание	В платформе Nova установлен таймаут запросов к Kubernetes API по умолчанию 1 мин. Данный параметр при необходимости должен корректироваться пользователем в зависимости от продолжительности и количества запросов к серверу Kubernetes API.	Пользователь Nova Container Platform
1.2.21	Ensure that the --service-account-lookup argument is set to true (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.22	Ensure that the --service-account-key-file argument is set as appropriate (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform

1.2.23	Ensure that the --etcd-certfile and --etcd-keyfile arguments are set as appropriate (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.24	Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.25	Ensure that the --client-ca-file argument is set as appropriate (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.26	Ensure that the --etcd-cafile argument is set as appropriate (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.27	Ensure that the --encryption-provider-config argument is set as appropriate (Manual)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.28	Ensure that encryption providers are appropriately configured (Manual)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.2.29	Ensure that the API Server only makes use of Strong Cryptographic Ciphers (Manual)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform

2.3. Конфигурация сервера Kubernetes Controller Manager

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
1.3.1	Ensure that the --terminated-pod-gc-threshold argument is set as appropriate (Manual)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.3.2	Ensure that the --profiling argument is set to false (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.3.3	Ensure that the --use-service-account-credentials argument is set to true (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.3.4	Ensure that the --service-account-private-key-file argument is set as appropriate (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform

1.3.5	Ensure that the --root-ca-file argument is set as appropriate (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.3.6	Ensure that the RotateKubeletServerCertificate argument is set to true (Automated)	2 (Мастер-узлы)	⚠️ Внимание	В Nova Container Platform сертификаты Kubelet создаются в отдельном защищенном PKI, размещаемом в компоненте StarVault. Поэтому ротация сертификатов средствами Controller Manager невозможна.	Nova Container Platform
1.3.7	Ensure that the --bind-address argument is set to 127.0.0.1 (Automated)	1 (Мастер-узлы)	⚠️ Внимание	В платформе Pod работает в `hostNetwork`. Это позволяет компоненту быть доступным внутри кластера для эффективного мониторинга и управления.	Nova Container Platform

2.4. Конфигурация сервера Kubernetes Scheduler

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
1.4.1	Ensure that the --profiling argument is set to false (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
1.4.2	Ensure that the --bind-address argument is set to 127.0.0.1 (Automated)	1 (Мастер-узлы)	⚠️ Внимание	В платформе Pod работает в `hostNetwork`. Это позволяет компоненту быть доступным внутри кластера для эффективного мониторинга и управления.	Nova Container Platform

3. Хранилище Etcd

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
2.1	Ensure that the --cert-file and --key-file arguments are set as appropriate (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
2.2	Ensure that the --client-cert-auth argument is set to true (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
2.3	Ensure that the --auto-tls argument is not set to true (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform

2.4	Ensure that the --peer-cert-file and --peer-key-file arguments are set as appropriate (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
2.5	Ensure that the --peer-client-cert-auth argument is set to true (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
2.6	Ensure that the --peer-auto-tls argument is not set to true (Automated)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
2.7	Ensure that a unique Certificate Authority is used for etcd (Manual)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform

4. Конфигурация Control Plane

4.1. Аутентификация и авторизация

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
3.1.1	Client certificate authentication should not be used for users (Manual)	1 (Мастер-узлы)	⚠️ Внимание	В платформе не используется данный метод аутентификации, для аутентификации пользователей используется протокол OIDC	Nova Container Platform
3.1.2	Service account token authentication should not be used for users (Manual)	2 (Мастер-узлы)	⚠️ Внимание	В платформе не используется данный метод аутентификации, для аутентификации пользователей используется протокол OIDC	Пользователь Nova Container Platform
3.1.3	Bootstrap token authentication should not be used for users (Manual)	1 (Мастер-узлы)	⚠️ Внимание	В платформе не используется данный метод аутентификации, для аутентификации пользователей используется протокол OIDC	Nova Container Platform

4.2. Логирование

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
3.2.1	Ensure that a minimal audit policy is created (Manual)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
3.2.2	Ensure that the audit policy covers key security concerns (Manual)	2 (Мастер-узлы)	✅ Соответствует		Пользователь Nova Container Platform

5. Конфигурация рабочих узлов

5.1. Конфигурационные файлы рабочих узлов

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
4.1.1	Ensure that the kubelet service file permissions are set to 600 or more restrictive (Automated)	1 (Рабочие узлы)	✅ Соответствует	При автоматизированной проверке по данному шагу может быть получен результат *Fail*. Это связано с тем, что проверка выполняется по пути `/etc/systemd/system/kubelet.service.d/10-kubeadm.conf` . В платформе файл конфигурации расположен по пути `/usr/lib/systemd/system/kubelet.service.d/10-kubeadm.conf` , права на который установлены в соответствие с рекомендацией.	Nova Container Platform
4.1.2	Ensure that the kubelet service file ownership is set to root:root (Automated)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform
4.1.3	If proxy kubeconfig file exists ensure permissions are set to 600 or more restrictive (Manual)	1 (Рабочие узлы)	⚠️ Внимание	При автоматизированной проверке по данному шагу может быть получен результат *Warn*. В платформе файл конфигурации лежит внутри подов, права на файл установлены в соответствие с рекомендацией.	Nova Container Platform
4.1.4	If proxy kubeconfig file exists ensure ownership is set to root:root (Manual)	1 (Рабочие узлы)	⚠️ Внимание	При автоматизированной проверке по данному шагу может быть получен результат *Warn*. В платформе файл конфигурации лежит внутри подов, владелец файла установлен в соответствие с рекомендацией.	Nova Container Platform
4.1.5	Ensure that the --kubeconfig kubelet.conf file permissions are set to 600 or more restrictive (Automated)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform
4.1.6	Ensure that the --kubeconfig kubelet.conf file ownership is set to root:root (Automated)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform

4.1.7	Ensure that the certificate authorities file permissions are set to 600 or more restrictive (Manual)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform
4.1.8	Ensure that the client certificate authorities file ownership is set to root:root (Manual)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform
4.1.9	If the kubelet config.yaml configuration file is being used validate permissions set to 600 or more restrictive (Manual)	2 (Рабочие узлы)	✅ Соответствует		Nova Container Platform
4.1.10	If the kubelet config.yaml configuration file is being used validate file ownership is set to root:root (Manual)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform

5.2. Конфигурация Kubelet

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
4.2.1	Ensure that the --anonymous-auth argument is set to false (Automated)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform
4.2.2	Ensure that the --authorization-mode argument is not set to AlwaysAllow (Automated)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform
4.2.3	Ensure that the --client-ca-file argument is set as appropriate (Automated)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform
4.2.4	Verify that the --read-only-port argument is set to 0 (Manual)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform
4.2.5	Ensure that the --streaming-connection-idle-timeout argument is not set to 0 (Manual)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform

4.2.6	Ensure that the --make-iptables-util-chains argument is set to true (Automated)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform
4.2.7	Ensure that the --hostname-override argument is not set (Manual)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform
4.2.8	Ensure that the eventRecordQPS argument is set to a level which ensures appropriate event capture (Manual)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform
4.2.9	Ensure that the --tls-cert-file and --tls-private-key-file arguments are set as appropriate (Manual)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform
4.2.10	Ensure that the --rotate-certificates argument is not set to false (Automated)	2 (Рабочие узлы)	⚠️ Внимание	В Nova Container Platform сертификаты Kubelet создаются в отдельном защищенном PKI, размещаемом в компоненте StarVault. Поэтому ротация сертификатов средствами Controller Manager невозможна.	Nova Container Platform
4.2.11	Verify that the RotateKubeletServerCertificate argument is set to true (Manual)	2 (Рабочие узлы)	✅ Соответствует	В Nova Container Platform сертификаты Kubelet создаются в отдельном защищенном PKI, размещаемом в компоненте StarVault. Поэтому ротация сертификатов средствами Controller Manager невозможна.	Nova Container Platform
4.2.12	Ensure that the Kubelet only makes use of Strong Cryptographic Ciphers (Manual)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform
4.2.13	Ensure that a limit is set on pod PIDs (Manual)	1 (Рабочие узлы)	⚠️ Внимание[1]		Nova Container Platform

5.3. Конфигурация Kube-proxy

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
4.3.1	Ensure that the kube-proxy metrics service is bound to localhost (Automated)	1 (Рабочие узлы)	✅ Соответствует		Nova Container Platform

6. Конфигурация политик

6.1. Конфигурация RBAC и сервисных аккаунтов

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
5.1.1	Ensure that the cluster-admin role is only used where required (Automated)	1 (Мастер-узлы)	⚠️ Внимание	Конфигурация компонентов платформы находится в зоне ответственности производителя. Конфигурация пользовательских компонентов, развернутых в платформе, находится в зоне ответственности администраторов платформы. Тест падает из-за того, что kubeadmins имеет bind к cluster-admin.	Совместно
5.1.2	Minimize access to secrets (Automated)	1 (Мастер-узлы)	✅ Соответствует	Конфигурация компонентов платформы находится в зоне ответственности производителя. Конфигурация пользовательских компонентов, развернутых в платформе, находится в зоне ответственности администраторов платформы.	Совместно
5.1.3	Minimize wildcard use in Roles and ClusterRoles (Automated)	1 (Мастер-узлы)	⚠️ Внимание	Конфигурация компонентов платформы находится в зоне ответственности производителя. Конфигурация пользовательских компонентов, развернутых в платформе, находится в зоне ответственности администраторов платформы. В платформе минимизорованы все Roles и ClusterRoles, которые используют маску ["*"], все роли с ["*"] либо служебные, либо необходимы.	Совместно
5.1.4	Minimize access to create pods (Automated)	1 (Мастер-узлы)	✅ Соответствует	Конфигурация компонентов платформы находится в зоне ответственности производителя. Конфигурация пользовательских компонентов, развернутых в платформе, находится в зоне ответственности администраторов платформы.	Совместно

5.1.5	Ensure that default service accounts are not actively used. (Automated)	1 (Мастер-узлы)	⚠️ Внимание	Конфигурация компонентов платформы находится в зоне ответственности производителя. Конфигурация пользовательских компонентов, развернутых в платформе, находится в зоне ответственности администраторов платформы.	Совместно
5.1.6	Ensure that Service Account Tokens are only mounted where necessary (Automated)	1 (Мастер-узлы)	⚠️ Внимание	Конфигурация компонентов платформы находится в зоне ответственности производителя. Конфигурация пользовательских компонентов, развернутых в платформе, находится в зоне ответственности администраторов платформы.	Совместно
5.1.7	Avoid use of `system:masters` group (Manual)	1 (Мастер-узлы)	⚠️ Внимание	Конфигурация компонентов платформы находится в зоне ответственности производителя. Конфигурация пользовательских компонентов, развернутых в платформе, находится в зоне ответственности администраторов платформы.	Совместно
5.1.8	Limit use of the Bind, Impersonate and Escalate permissions in the Kubernetes cluster (Manual)	1 (Мастер-узлы)	⚠️ Внимание	Конфигурация компонентов платформы находится в зоне ответственности производителя. Конфигурация пользовательских компонентов, развернутых в платформе, находится в зоне ответственности администраторов платформы.	Совместно
5.1.9	Minimize access to create persistent volumes (Manual)	1 (Мастер-узлы)	⚠️ Внимание	Конфигурация компонентов платформы находится в зоне ответственности производителя. Конфигурация пользовательских компонентов, развернутых в платформе, находится в зоне ответственности администраторов платформы.	Совместно

5.1.10	Minimize access to the proxy sub-resource of nodes (Manual)	1 (Мастер-узлы)	⚠️ Внимание	Конфигурация компонентов платформы находится в зоне ответственности производителя. Конфигурация пользовательских компонентов, развернутых в платформе, находится в зоне ответственности администраторов платформы.	Совместно
5.1.11	Minimize access to the approval sub-resource of `certificatesigningrequests` objects (Manual)	1 (Мастер-узлы)	⚠️ Внимание	Конфигурация компонентов платформы находится в зоне ответственности производителя. Конфигурация пользовательских компонентов, развернутых в платформе, находится в зоне ответственности администраторов платформы.	Совместно
5.1.12	Minimize access to webhook configuration objects (Manual)	1 (Мастер-узлы)	⚠️ Внимание	Конфигурация компонентов платформы находится в зоне ответственности производителя. Конфигурация пользовательских компонентов, развернутых в платформе, находится в зоне ответственности администраторов платформы.	Совместно
5.1.13	Minimize access to the service account token creation (Manual)	1 (Мастер-узлы)	⚠️ Внимание	Конфигурация компонентов платформы находится в зоне ответственности производителя. Конфигурация пользовательских компонентов, развернутых в платформе, находится в зоне ответственности администраторов платформы.	Совместно

6.2. Конфигурация Pod Security Standards

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности

5.2.1	Ensure that the cluster has at least one active policy control mechanism in place (Manual)	1 (Мастер-узлы)	⚠ Внимание	В Nova Container Platform по умолчанию ко всем системным пространствам имен (*namespace*) применяются политики Pod Security Standards. Уровень безопасности каждой политики установлен в зависимости от требований размещаемого в пространстве имен компонента платформы. Дополнительные политики и правила могут быть сконфигурированы пользователем при необходимости с помощью инструментов системы безопасности Neuvector.	Совместно
5.2.2	Minimize the admission of privileged containers (Manual)	1 (Мастер-узлы)	⚠ Внимание	В Nova Container Platform по умолчанию ко всем системным пространствам имен (*namespace*) применяются политики Pod Security Standards. Уровень безопасности каждой политики установлен в зависимости от требований размещаемого в пространстве имен компонента платформы. Дополнительные политики и правила могут быть сконфигурированы пользователем при необходимости с помощью инструментов системы безопасности Neuvector.	Совместно
5.2.3	Minimize the admission of containers wishing to share the host process ID namespace (Manual)	1 (Мастер-узлы)	⚠ Внимание	В Nova Container Platform по умолчанию ко всем системным пространствам имен (*namespace*) применяются политики Pod Security Standards. Уровень безопасности каждой политики установлен в зависимости от требований размещаемого в пространстве имен компонента платформы. Дополнительные политики и правила могут быть сконфигурированы пользователем при необходимости с помощью инструментов системы безопасности Neuvector.	Совместно

5.2.4	Minimize the admission of containers wishing to share the host IPC namespace (Manual)	1 (Мастер-узлы)	⚠️ Внимание	В Nova Container Platform по умолчанию ко всем системным пространствам имен (*namespace*) применяются политики Pod Security Standards. Уровень безопасности каждой политики установлен в зависимости от требований размещаемого в пространстве имен компонента платформы. Дополнительные политики и правила могут быть сконфигурированы пользователем при необходимости с помощью инструментов системы безопасности Neuvector.	Совместно
5.2.5	Minimize the admission of containers wishing to share the host network namespace (Manual)	1 (Мастер-узлы)	⚠️ Внимание	В Nova Container Platform по умолчанию ко всем системным пространствам имен (*namespace*) применяются политики Pod Security Standards. Уровень безопасности каждой политики установлен в зависимости от требований размещаемого в пространстве имен компонента платформы. Дополнительные политики и правила могут быть сконфигурированы пользователем при необходимости с помощью инструментов системы безопасности Neuvector.	Совместно
5.2.6	Minimize the admission of containers with `allowPrivilegeEscalation` (Manual)	1 (Мастер-узлы)	⚠️ Внимание	В Nova Container Platform по умолчанию ко всем системным пространствам имен (*namespace*) применяются политики Pod Security Standards. Уровень безопасности каждой политики установлен в зависимости от требований размещаемого в пространстве имен компонента платформы. Дополнительные политики и правила могут быть сконфигурированы пользователем при необходимости с помощью инструментов системы безопасности Neuvector.	Совместно

5.2.7	Minimize the admission of root containers (Manual)	1 (Мастер-узлы)	⚠ Внимание	В Nova Container Platform по умолчанию ко всем системным пространствам имен (*namespace*) применяются политики Pod Security Standards. Уровень безопасности каждой политики установлен в зависимости от требований размещаемого в пространстве имен компонента платформы. Дополнительные политики и правила могут быть сконфигурированы пользователем при необходимости с помощью инструментов системы безопасности Neuvector.	Совместно
5.2.8	Minimize the admission of containers with the NET_RAW capability (Manual)	1 (Мастер-узлы)	⚠ Внимание	В Nova Container Platform по умолчанию ко всем системным пространствам имен (*namespace*) применяются политики Pod Security Standards. Уровень безопасности каждой политики установлен в зависимости от требований размещаемого в пространстве имен компонента платформы. Дополнительные политики и правила могут быть сконфигурированы пользователем при необходимости с помощью инструментов системы безопасности Neuvector.	Совместно
5.2.9	Minimize the admission of containers with added capabilities (Manual)	1 (Мастер-узлы)	⚠ Внимание	В Nova Container Platform по умолчанию ко всем системным пространствам имен (*namespace*) применяются политики Pod Security Standards. Уровень безопасности каждой политики установлен в зависимости от требований размещаемого в пространстве имен компонента платформы. Дополнительные политики и правила могут быть сконфигурированы пользователем при необходимости с помощью инструментов системы безопасности Neuvector.	Совместно

5.2.10	Minimize the admission of containers with capabilities assigned (Manual)	2 (Мастер-узлы)	⚠ Внимание	В Nova Container Platform по умолчанию ко всем системным пространствам имен (*namespace*) применяются политики Pod Security Standards. Уровень безопасности каждой политики установлен в зависимости от требований размещаемого в пространстве имен компонента платформы. Дополнительные политики и правила могут быть сконфигурированы пользователем при необходимости с помощью инструментов системы безопасности Neuvector.	Совместно
5.2.11	Minimize the admission of Windows HostProcess containers (Manual)	1 (Мастер-узлы)	⚠ Внимание	В Nova Container Platform по умолчанию ко всем системным пространствам имен (*namespace*) применяются политики Pod Security Standards. Уровень безопасности каждой политики установлен в зависимости от требований размещаемого в пространстве имен компонента платформы. Дополнительные политики и правила могут быть сконфигурированы пользователем при необходимости с помощью инструментов системы безопасности Neuvector.	Совместно
5.2.12	Minimize the admission of HostPath volumes (Manual)	1 (Мастер-узлы)	⚠ Внимание	В Nova Container Platform по умолчанию ко всем системным пространствам имен (*namespace*) применяются политики Pod Security Standards. Уровень безопасности каждой политики установлен в зависимости от требований размещаемого в пространстве имен компонента платформы. Дополнительные политики и правила могут быть сконфигурированы пользователем при необходимости с помощью инструментов системы безопасности Neuvector.	Совместно

5.2.13	Minimize the admission of containers which use HostPorts (Manual)	1 (Мастер-узлы)	⚠️ Внимание	В Nova Container Platform по умолчанию ко всем системным пространствам имен (*namespace*) применяются политики Pod Security Standards. Уровень безопасности каждой политики установлен в зависимости от требований размещаемого в пространстве имен компонента платформы. Дополнительные политики и правила могут быть сконфигурированы пользователем при необходимости с помощью инструментов системы безопасности Neuvector.	Совместно

6.3. Конфигурация сетевых политик и CNI

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
5.3.1	Ensure that the CNI in use supports NetworkPolicies (Manual)	1 (Мастер-узлы)	✅ Соответствует		Nova Container Platform
5.3.2	Ensure that all Namespaces have Network Policies defined (Manual)	2 (Мастер-узлы)	⚠️ Внимание	По умолчанию в Nova Container Platform нет предустановленных сетевых политик для системных компонентов и пространств имен во избежание конфликтов и избыточной конфигурации правил сетевой безопасности. В системе безопасности Neuvector выполняется постоянное сканирование сетевой активности всех компонентов кластера, на основании которого автоматически создаются необходимые правила. Пользователь может в любой момент изменить режим работы данных правил. Поддерживается три режима работы: обнаружение, мониторинг и защита.	Совместно

6.4. Управление секретами

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
5.4.1	Prefer using secrets as files over secrets as environment variables (Manual)	2 (Мастер-узлы)	✅ Соответствует		Совместно

5.4.2	Consider external secret storage (Manual)	2 (Мастер-узлы)	✅ Соответствует		Совместно

6.5. Расширенная конфигурация Admission Control

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
5.5.1	Configure Image Provenance using ImagePolicyWebhook admission controller (Manual)	2 (Мастер-узлы)	⚠️ Внимание	Admission-вебхуки, реализующие функционал контроля образов, могут быть сконфигурированы пользователем при необходимости с помощью инструментов системы безопасности Neuvector.	Nova Container Platform

6.6. Общие рекомендации

Пункт	Рекомендация	Уровень	Результат	Комментарий	Зона ответственности
5.6.1	Create administrative boundaries between resources using namespaces (Manual)	2 (Мастер-узлы)	✅ Соответствует		Совместно
5.6.2	Ensure that the seccomp profile is set to docker/default in your pod definitions (Manual)	2 (Мастер-узлы)	⚠️ Внимание[2]		Совместно
5.6.3	Apply SecurityContext to your Pods and Containers (Manual)	2 (Мастер-узлы)	✅ Соответствует		Совместно
5.6.4	The default namespace should not be used (Manual)	2 (Мастер-узлы)	✅ Соответствует		Совместно

1. Автоматическая установка параметров `podPidsLimit` и `maxPods` в конфигурации Kubelet доступна в Nova Container Platform версии v2.0.0 и выше.
2. Установка профилей seccomp для системных компонентов доступна в Nova Container Platform версии v2.0.0 и выше.

Nova Container Platform

Данный раздел содержит историю изменений Nova Container Platform.

История изменений

- v7
- v6
- v5
- v4
- Архивные версии:
  - v3

История изменений

Данный раздел содержит историю изменений Nova Universe.

Содержание раздела