Part XIX: Security in Informix

Tables of Contents

Security in Informix

Informix on Red Hat OpenShift supports Socker Secure Security (SSL) to encrypt data in transit.

In addition, client-server communications can be fully encrypted at both the network and disk level.

SCC Capabilities

The security context constraints (SCC) for Informix have the following capabilities:

SYS_RESOURCE
: Allows manipulation of reservations, memory allocations and resource limits. Maximum memory allocation is still constrained by the memory cgroup (memcg) limit which cannot be overridden by this sys-capability. The Informix database engine needs this sys-capability to increase the resource limits (IE.ulimits).

IPC_OWNER
: Bypasses permission checks for operations on IPC objects. Even when the IPC kernel parameters are set to maximum values on the hosts/worker nodes, the Informix engine still tries to dynamically throttle those values. This system capability is provided in addition to sharing IPC namespace with the host.

SYS_NICE
: Allows changing process priorities. Because each container has its own PID namespace, this capability only applies to that container. The Informix database engine relies on process thread prioritization to ensure that Work Load Management (WLM) and Fast Communications Manager (FCM) processing is prioritized over generic agent work.

CHOWN
: Necessary to run chown to change ownership of files/directories in persistent volumes.

DAC_OVERRIDE
: Bypasses permission checks for file read, write, and execute.

FSETID
: Prevents the clearing of the setuid and setgid mode bits when a file is modified.

FOWNER
: Bypasses permission checks on operations that normally require the filesystem UID of the process to match the UID of the file (for example, chmod(2), utime(2)), excluding those operations that are covered by CAP_DAC_OVERRIDE and CAP_DAC_READ_SEARCH.

SETGID
: Necessary to run Informix engine processes with escalated group privileges.

SETUID
: Necessary to run Informix engine processes with escalated user privileges.

SETFCAP
: Used to set capabilities on files.

SETPCAP
: Used to set capabilities on processes.

SYS_CHROOT
: Necessary to use the chroot command.

KILL
: Bypasses permission checks for sending signals. Necessary for signal handling during process management.

AUDIT_WRITE

Required to write records to the kernel auditing log when SELinux is enabled.

Role-binding access control

The informix ServiceAccount and associated informix-cr Role are necessary for pod-to-pod control and communication for a successful deployment. The resources and verbs are outlined below:

```
rules:
- apiGroups: [""]
  resources: ["pods", "pods/log", "pods/exec"]
  verbs: ["get", "list", "patch", "watch", "update", "create"]

- apiGroups: [""]
  resources: ["services"]
  verbs: ["get", "list"]

- apiGroups: ["batch", "extensions"]
  resources: ["jobs", "deployments"]
  verbs: ["get", "list", "watch", "patch"]
```

Hostpath requirements

The /proc and /proc/sys volumes must be mounted into an init container to either set or validate the required IPC kernel parameters for Informix. Hostpath volumes are also supported for single-node Informix deployments.