
watchdog

service watchdog

Description

Le noyau linux peut réinitialiser le système si des problèmes sérieux sont détectés. Cela peut être implémenté via le hardware spécial watchdog, ou via un watchdog logiciel légèrement moins fiable dans le kernel. Dans tous les cas, un service doit dire au kernel que tout va bien. Si le service ne le fait plus, le système est réinitialisé.

Watchdog est un service qui ouvre **/dev/watchdog**, et maintient une écriture aussi souvent que possible pour empêcher le noyau de se réinitialiser, au moins une fois par minute. Chaque écriture retarde le temps de reboot d'une minute. Au bout d'une minute d'inactivité, le système est réinitialisé. Dans le cas d'un watchdog logiciel, la capacité de rebooter le système dépend de l'état de la machines et des interruptions.

Le service watchdog peut être stoppé sans reboot si le périphérique **/dev/watchdog** est fermé correctement, sauf si le kernel a été compilé avec l'option `CONFIG_WATCHDOG_NOWAYOUT`.

Tests

Le service Watchdog effectue de nombreux tests pour vérifier le status du système :

- Est-ce que la table des processus est pleine ?
- Y'a t'il suffisamment de mémoire vive ?
- Y'a t'il suffisamment de mémoire allouable ?
- Est-ce que certains fichiers sont accessibles ?
- Est-ce que certains fichiers ont changés dans l'intervalle de temps donné ?
- Est-ce que la charge système est trop élevée ?
- Est-ce qu'un débordement de table de fichier se produit ?
- Est-ce qu'un processus fonctionne (identifié par un fichier pid) ?
- Est-ce qu'une adresse IP répond aux ping ?
- Est-ce que les interfaces réseaux reçoivent du trafic ?
- Est-ce que la température est trop élevée ?
- Exécute une commande utilisateur pour effectuer des tests arbitraires.
- Exécute une commande de test/réparation.

Si une de ces vérifications échouent, le système s'éteint. Si un de ces tests, excepté les commandes utilisateurs, dépassent une minute, la machine est redémarrée.

OPTIONS

-
- v, **-verbose** mode verbeux
 - s, **-sync** tente de synchroniser le système de fichier à chaque fois que le processus est réveillé.
 - b, **-softboot** soft boot le système si une erreur se produit durant la boucle principale. par ex, si un fichier n'est pas accessible via l'appel stat(). Ne s'applique pas à /dev/watchdog et /proc/loadavg.
 - F, **-foreground** Ne passe pas en tâche de fond
 - f, **-force** Force l'utilisation de l'intervalle donné ou la charge moyenne maximale dans la configuration.
 - c **config-file**, **-config-file config-file** Spécifie le fichier de configuration au lieu du défaut /etc/watchdog.conf
 - q, **-no-action** Ne reboot pas et n'arrête pas la machine.

Fonctions

Une fois watchdog démarré, il se place en tâche de fond et tente toutes les vérifications spécifiées dans sa configuration. Entre chaque test il écrit dans le périphérique kernel pour empêcher un reset. Une fois tous les tests terminés, watchdog s'endort un certain temps. Le périphérique kernel s'attend à une écriture par minute pour empêcher un reset. Par défaut, watchdog est lancé toutes les secondes pour gérer le périphérique le plus tôt possible.

Sous de forte charges système, watchdog peut avoir été swappé et peut échouer à revenir à temps. Dans ce cas le kernel va réinitialiser la machine. l'option **realtime** s'assure qu'il ne sera jamais swappé. Sur les systèmes n'ayant plus de mémoire vive disponible, le kernel va tenter de libérer de la mémoire en tuant des processus. watchdog est exempt de ce système.

Watchdog tente également périodiquement de se forker lui-même pour voir si la table des processus n'est pas pleine. Ce processus va laisser un processus zombie jusqu'à ce que watchdog se réveille, c'est un fonctionnement normal.

Soft reboot

Un soft reboot (shutdown et reboot contrôlé) est initié pour toute erreur qui est trouvée. Vu qu'il peut ne plus y avoir d'autres processus disponibles, watchdog fait tout par lui-même. Cela signifie :

1. Tuer tous les processus avec un SIGTERM
2. Tuer tous les processus restant avec un SIGKILL
3. Enregistre un shutdown dans wtmp
4. Sauve la valeur aléatoire de /dev/urandom si possible
5. Désactive l'accounting
6. Désactive les quota et le swap
7. Démonte toutes les partitions sauf /
8. Remonte root en lecture-seule
9. Éteins toutes les interfaces réseaux
10. Reboot

Binaire de vérification

Si le code de retour du binaire de vérification n'est pas 0, watchdog assume une erreur et reboot le système. Les valeurs de retour suivants ont une signification particulière :

- 255 Reboot le système.
- 254 Réinitialise le système

-
- 253 Surcharge système
 - 252 Température trop élevée
 - 251 /proc/loadavg ne contient pas de données (ou trop peu)
 - 250 Le fichier donné n'a pas été changé dans l'intervalle donné
 - 249 /proc/meminfo contient des données invalides
 - 248 Processus enfant tué par un signal
 - 247 Processus enfant n'a pas retourné dans le temps imparti
 - 246 libre pour une utilisation spécifique
 - 245 Réservé pour un résultat inconnu.

Binaire repair

Le binaire repair est lancé avec un paramètre : le numéro d'erreur qui a causé watchdog d'initier le processus de boot. Après avoir tenté de réparer le système le binaire devrait quitter avec le code 0 si le système à été réparé avec succès, sinon watchdog reboot. Le code de retour devrait être le code d'erreur qui cause watchdog a rebooter.

Répertoire test

Les exécutable dans le répertoire de test sont découverts par watchdog au démarrage et sont automatiquement exécutés. Ces exécutable sont appelé soit avec "test" comme premier argument (si un test est effectué), ou "repair" (si une réparation pour un test précédent doit être effectué). Si une opération de test échoue, le même exécutable est appelé avec l'argument repair avec le code de retour de l'opération précédente en tant que second argument.

Fichiers

- /etc/watchdog.conf** Fichier de configuration de watchdog
- /etc/watchdog.d** répertoire contenant les commandes test ou repair.