Sun™ Control Station 2.2
Module Contrôle de l'intégrité

Sun Microsystems, Inc.
www.sun.com

Référence : 819-1421-10
Décembre 2004 Révision A

Envoyez vos commentaires concernant ce document à l'adresse : `http://www.sun.com/hwdocs/feedback`

Papier
recyclable

Adobe PostScript

Table des matières

Module Contrôle de l'intégrité

Le module Contrôle de l'intégrité de Sun™ Control Station permet de contrôler le statut de divers paramètres des hôtes gérés. Ce document présente les fonctions et services disponibles dans ce module, grâce auxquels vous pouvez :

- afficher un récapitulatif des informations sur l'intégrité d'un hôte ou d'un groupe d'hôtes ;
- extraire les données de statut d'intégrité les plus récentes à partir des hôtes gérés ;
- planifier les requêtes à adresser aux hôtes gérés afin de recueillir les données de statut d'intégrité ;
- vérifier que vous pouvez contacter l'agent résidant sur un hôte géré spécifique et que cet hôte est accessible sur le réseau ;
- forcer la station de contrôle à extraire immédiatement les données de statut d'intégrité les plus récentes sur un hôte individuel ;
- configurer les paramètres du module Contrôle de l'intégrité ;
- saisir l'adresse e-mail à laquelle le module Contrôle de l'intégrité enverra les alertes en cas d'événements système critiques (représentés par un point d'exclamation sur un cercle jaune ou par une croix sur un cercle rouge).

Remarque – ce manuel part du principe que vous connaissez le fonctionnement de base du logiciel Sun Control Station. Pour une présentation des fonctions de base de Sun Control Station, telles que les icônes de statut, la fenêtre de sélection, l'ordonnanceur et la boîte de dialogue Progression de la tâche, reportez-vous à la documentation *Sun Control Station 2.2 – Manuel de l'administrateur*.

Contrôle des hôtes gérés

Les opérations de contrôle du module Contrôle de l'intégrité sont basées sur une série de requêtes et d'événements. Cela signifie que les données relatives au statut de l'intégrité sont acquises soit par la station de contrôle qui lance une requête pour lire les informations sur l'état du client pour chaque hôte, soit par l'hôte géré qui informe immédiatement la station de contrôle dès qu'un problème (un *événement*) est détecté.

La FIGURE 1 illustre les tableaux Événements critiques et Statut du groupe d'hôtes gérés.

FIGURE 1 Tableaux de contrôle de l'intégrité

Dans les tableaux de contrôle de l'intégrité, l'horodatage indiqué pour un événement correspond à l'heure de la dernière modification de son statut, par exemple de l'état jaune à l'état rouge.

Alertes de contrôle de l'intégrité

Si un événement critique est détecté sur la station de contrôle, une alerte de statut s'affiche dans l'angle supérieur gauche de l'interface utilisateur. Un événement critique est généré lors de la transition entre un état "avertissement" et un état "critique", c'est-à-dire lorsqu'un état jaune ou rouge est renvoyé suite à une requête d'intégrité.

Un événement critique peut impliquer tout type de services ou de composants matériels sur un hôte géré.

Problèmes connus

Cette section présente les difficultés qui peuvent surgir lors de l'utilisation du module Contrôle de l'intégrité, notamment lorsqu'un hôte est géré par plusieurs stations de contrôle.

Paramètres conflictuels

Les paramètres du module Contrôle de l'intégrité (les seuils d'alarmes d'UC, par exemple) peuvent être modifiés à partir de toute station de contrôle. Lorsque l'on modifie ces paramètres sur une station de contrôle, les nouvelles valeurs sont propagées à tous les hôtes gérés de cette station de contrôle.

En cas de modification, tous les paramètres existants des hôtes gérés sont systématiquement remplacés par les nouvelles valeurs. Cependant, les paramètres qui s'affichent dans les interfaces de l'autre station de contrôle ne sont pas mis à jour et, par conséquent, ne reflètent pas les changements.

Pour des résultats optimaux, si plus d'une station de contrôle gère un hôte donné, assurez-vous que les paramètres de contrôle de l'intégrité sont les mêmes sur chaque station de contrôle.

Informations LOM inattendues dans le module Contrôle de l'intégrité

Ce problème survient lorsqu'un hôte est géré par deux stations de contrôle ou davantage *et que* :

- Le module de contrôle LOM est installé sur une station de contrôle uniquement.
- Le logiciel client du module de contrôle LOM est installé sur l'hôte géré.

Le module Contrôle de l'intégrité étant conçu pour recevoir des informations LOM lorsqu'elles sont disponibles, les tableaux de contrôle de l'intégrité de toutes les stations de contrôle affichent donc eux aussi ces informations, même si le module de contrôle LOM n'a pas été installé sur toutes les stations de contrôle.

Il ne s'agit ni d'un bogue ni d'un dysfonctionnement. Cela signifie simplement que vous risquez de voir des informations LOM s'afficher dans les tableaux de contrôle de l'intégrité alors que vous ne vous y attendez pas.

Écran Contrôle de l'intégrité

Pour afficher ou mettre à jour le statut actuel des services et des composants matériels des hôtes gérés, cliquez sur l'option de menu Contrôle de l'intégrité, puis sur l'option de sous-menu correspondante.

Les options de sous-menu disponibles sont les suivantes :

- Récapitulatif de l'intégrité (voir “Récapitulatif de l'intégrité” on page 5) ;
- Afficher les hôtes (voir “Affichage du récapitulatif de l'intégrité de tous les hôtes” on page 9) ;
- Paramètres (voir “Paramètres” on page 11).

Récapitulatif de l'intégrité

L'option de sous-menu Récapitulatif de l'intégrité affiche un récapitulatif des données de statut d'intégrité des hôtes gérés.

Lorsque vous cliquez sur l'option de sous-menu Récapitulatif de l'intégrité, les tableaux Événements critiques et Statut du groupe d'hôtes gérés s'affichent (voir FIGURE 1).

- Le tableau Événements critiques affiche les événements que l'administrateur devrait traiter immédiatement.
- Le tableau Statut du groupe d'hôtes gérés affiche le statut général des groupes d'hôtes figurant sur la station de contrôle.

Lorsque vous cliquez sur une icône en forme de *loupe* pour afficher des informations plus détaillées sur un hôte, trois tableaux s'affichent :

- Le tableau Composants système principaux, qui affiche des informations sur l'UC, le disque, la mémoire et le réseau.
- Le tableau Services principaux, qui affiche les informations sur les différents services en cours sur cet hôte spécifique, par exemple sur les serveurs FTP, Telnet, DNS ou le serveur d'e-mail (ces éléments peuvent varier selon le type d'hôte affiché).
- Le tableau Autres services système, qui affiche des informations sur les services de tiers ou services personnalisés que l'administrateur a ajoutés à un hôte.

Remarque – pour ajouter un nouveau service de contrôle de l'intégrité, reportez-vous à la section “Ajout de nouveaux services au module Contrôle de l'intégrité” on page 16.

Affichage des données de contrôle d'intégrité

Pour afficher un récapitulatif des données de contrôle d'intégrité sur un hôte géré :

1. **Sélectionnez Contrôle de l'intégrité → Récapitulatif de l'intégrité.**

   Les tableaux Événements critiques et Statut du groupe d'hôtes gérés s'affichent.

2. **Pour afficher plus d'informations sur un événement critique, cliquez dans la colonne Action sur l'icône en forme de *loupe* située en regard de l'élément.**

   Les tableaux suivants s'affichent (voir FIGURE 2) :

FIGURE 2 Tableaux détaillés

- Composants système principaux
- Services principaux
- Autres services système

Pour revenir à l'écran précédent, cliquez sur l'icône de la *flèche vers le haut* dans l'angle supérieur droit.

3. **Si vous visualisez les détails d'un groupe d'hôtes gérés, le tableau État des hôtes gérés s'affiche. Il répertorie les hôtes appartenant à ce groupe.**

   Dans la colonne Action, vous pouvez cliquer sur l'icône en forme de *loupe* située en regard de l'hôte. Les trois tableaux détaillés mentionnés précédemment s'affichent.

   Pour revenir à l'écran précédent, cliquez sur l'icône de la *flèche vers le haut* dans l'angle supérieur droit.

Tableau Événements critiques : bouton Actualiser

Au-dessus du tableau Événements critiques figure le bouton Actualiser. Il permet la mise à jour instantanée de la fenêtre de l'interface utilisateur, de façon à refléter les dernières modifications de la base de données.

Ce bouton ne permet pas de mettre à jour la base de données avec de nouvelles informations provenant des hôtes gérés. Pour mettre à jour les informations qui figurent dans la base de données, reportez-vous à la section “Mise à jour des données sur le statut de l'intégrité” on page 8.

Services contrôlés sur les hôtes gérés

Parmi les services contrôlés sur les hôtes gérés figurent :

- le serveur DNS ;
- le serveur d'e-mail ;
- le serveur FTP ;
- le serveur MySQL ;
- le serveur SSH ;
- le serveur Telnet ;
- le serveur Web.

Suppression des événements critiques

Les événements critiques qui surviennent sur un hôte géré s'affichent dans le tableau Événements critiques. Si vous choisissez de ne pas traiter un événement critique donné, vous pouvez l'effacer du tableau. Cette opération ne supprime pas le problème de l'hôte géré, mais elle garantit que plus aucune notification ne sera émise à ce sujet dans le tableau Événements critiques.

Remarque – si un événement critique signalant un autre problème est généré sur le même hôte géré, un nouvel événement critique s'affiche dans le tableau.

Pour effacer du tableau Événements critiques un seul ou tous les événements critiques :

1. **Sélectionnez Contrôle de l'intégrité → Récapitulatif de l'intégrité.**

   Les tableaux Événements critiques et Statut du groupe d'hôtes gérés s'affichent.

2. **Pour effacer un événement critique du tableau, cliquez dans la colonne Action sur l'icône de *suppression* située en regard de cet événement.**

   Le tableau Événements critiques est mis à jour et reflète la suppression de cet événement.

3. **Pour effacer du tableau tous les événements critiques, cliquez au-dessus du tableau sur Effacer les événements critiques.**

   Le tableau Événements critiques est mis à jour et ne contient plus aucune entrée.

Mise à jour des données sur le statut de l'intégrité

Vous pouvez actualiser les données relatives au statut de l'intégrité de chaque hôte. Cette fonction permet à la station de contrôle d'extraire immédiatement les données de statut d'intégrité les plus récentes d'un hôte individuel.

Le bouton Mettre à jour maintenant s'affiche dans l'interface utilisateur lorsque vous affichez les tableaux détaillés d'un hôte spécifique. Pour actualiser les données de statut d'intégrité sur un hôte géré :

1. **Sélectionnez Contrôle de l'intégrité → Récapitulatif de l'intégrité.**

   Les tableaux Événements critiques et Statut du groupe d'hôtes gérés s'affichent.

2. **Cliquez dans la colonne Action sur l'icône en forme de *loupe* située en regard de l'élément.**

   Les tableaux détaillés s'affichent.

3. **Si vous visualisez les détails d'un événement critique, les tableaux détaillés ci-dessous s'affichent :**
   - Composants système principaux
   - Services principaux
   - Autres services système
4. **Si vous visualisez les détails d'un groupe d'hôtes gérés, le tableau État des hôtes gérés s'affiche. Il répertorie les hôtes appartenant à ce groupe.**

   Dans la colonne Action, vous pouvez cliquer sur l'icône en forme de *loupe* située en regard de l'hôte. Les trois tableaux détaillés mentionnés précédemment s'affichent.
5. **Dans la fenêtre affichant les tableaux détaillés d'un hôte, cliquez au-dessus du tableau sur Mettre à jour maintenant.**

   Cette opération force la station de contrôle à extraire immédiatement les données d'intégrité de l'hôte géré.

   La boîte de dialogue Progression de la tâche s'affiche.
6. **Pour revenir à l'écran précédent, cliquez sur l'icône de la *flèche vers le haut* dans l'angle supérieur droit.**

Affichage du récapitulatif de l'intégrité de tous les hôtes

Pour afficher l'intégrité générale de chaque hôte géré dans un seul tableau :

1. **Sélectionnez Contrôle de l'intégrité → Afficher les hôtes.**

   Le tableau État des hôtes gérés s'affiche et dresse la liste des hôtes gérés (voir FIGURE 3).

FIGURE 3 Tableau État des hôtes gérés

Remarque – si le tableau État des hôtes gérés contient plus de dix entrées, seules les dix premières s'affichent. Les boutons situés dans la partie inférieure permettent de sélectionner les différentes plages d'entrées.

2. **Pour afficher plus d'informations sur un hôte spécifique, cliquez dans la colonne Action sur l'icône en forme de *loupe* située en regard de cet hôte.**

   Les tableaux détaillés suivants s'affichent :

   - Composants système principaux
   - Services principaux
   - Autres services système

   Pour revenir à l'écran précédent, cliquez sur l'icône de la *flèche vers le haut* dans l'angle supérieur droit.

3. **Dans l'écran affichant les tableaux détaillés d'un hôte, cliquez sur Mettre à jour maintenant.**

   Cette opération force la station de contrôle à extraire immédiatement les données d'intégrité de l'hôte géré.

   La boîte de dialogue Progression de la tâche s'affiche.

4. **Pour revenir à l'écran précédent, cliquez sur l'icône de la *flèche vers le haut* dans l'angle supérieur droit.**

Actualisation de l'interface utilisateur

- **Cliquez sur le bouton Actualiser.**

  Ce bouton, situé au-dessus du tableau État des hôtes gérés, lance l'actualisation automatique de l'interface afin de refléter les dernières modifications de la base de données.

  Ce bouton ne permet pas de mettre à jour la base de données avec de nouvelles informations provenant des hôtes gérés.

Paramètres

Requête de vérification d'activité

Cette fonction permet à la station de contrôle de vérifier que l'agent est toujours en cours d'exécution sur un hôte géré et que ce dernier est accessible sur le réseau. Elle fonctionne de la manière suivante :

1. La station de contrôle envoie une requête simple sur l'agent.

   Si la requête est fructueuse, cela signifie que l'agent fonctionne normalement et que l'hôte est accessible sur le réseau. Le statut du composant réseau est signalé en vert dans le tableau Composants système principaux.

   Si la requête est infructueuse, le statut du composant réseau devient rouge (voir l'exemple de la FIGURE 2).

2. Une commande ping est alors envoyée à l'hôte dont l'agent est en échec afin de vérifier la connexion réseau, via le protocole ICMP (Internet Control Message Protocol).

   Si ce ping ICMP est fructueux, le tableau des informations sur le contrôle de l'intégrité dans la base de données signale que la station de contrôle ne peut pas accéder à l'agent à l'*adresse IP* de l'hôte.

   Si en revanche ce ping ICMP échoue, le tableau signale que la station de contrôle ne peut pas accéder à l'*adresse IP* de l'hôte sur le réseau.

Requête sur le statut

L'intervalle de requête sur le statut indique le début d'un cycle de requête (toutes les quatre heures, par exemple) dans le cadre de l'extraction des données d'intégrité à partir des hôtes gérés.

Lors de la configuration de cet intervalle, vous devez prendre en considération le nombre d'hôtes gérés par la station de contrôle. Les hôtes gérés sont interrogés en série. Lorsque la station de contrôle détecte un hôte inaccessible (y compris les défaillances de l'agent SCS), le temps de réponse à la requête de statut est de dix (10) minutes maximum.

Si la station de contrôle détecte plusieurs hôtes inaccessibles pendant un cycle d'interrogation, un cycle donné peut ne pas être terminé au moment du démarrage du cycle d'interrogation suivant.

L'intervalle minimal entre les requêtes de statut est d'une heure. Si Sun Control Station gère plusieurs hôtes, choisissez un intervalle plus long.

Paramètres des requêtes de statut et d'activité

Vous pouvez configurer les paramètres des requêtes de statut et d'activité suivants :

- **Intervalle d'exécution :** définissez l'intervalle auquel la station de contrôle doit essayer de communiquer avec les hôtes gérés, par exemple toutes les six (6) heures.
- **Minute(s) d'exécution :** sélectionnez la ou les minutes auxquelles vous souhaitez exécuter la requête de vérification d'activité. Mettez les minutes en évidence et utilisez les touches fléchées pour les déplacer d'une fenêtre de défilement à l'autre.
- **Adresse e-mail :** saisissez l'adresse e-mail de la personne qui sera notifiée de l'exécution de la requête de vérification d'activité.
- **Notifier au début :** cochez cette case pour informer la personne du démarrage de la tâche.
- **Notifier à la fin :** cochez cette case pour informer la personne de la fin de la tâche.

Paramètres de contrôle d'intégrité configurables

Vous pouvez configurer les paramètres suivants :

- **Activer les événements :** si vous cochez cette case, tous les hôtes gérés envoient tous les événements générés sur les hôtes à la station de contrôle. Dans le cas contraire, aucun événement n'est envoyé à la station de contrôle.

  Les événements parviennent à la station de contrôle via le port 80.

  Cette fonction n'a pas d'incidence sur les événements détectés lors d'un intervalle de requête.
- **Adresse e-mail de notification :** il s'agit de l'adresse e-mail à laquelle le module Contrôle de l'intégrité envoie des alertes lorsque des événements système critiques sont détectés (cercle rouge).

  Vous ne pouvez saisir qu'une adresse e-mail dans ce champ.

Remarque – lors de l'ajout d'un hôte à la station de contrôle, si vous indiquez l'adresse e-mail de l'administrateur de cet hôte, le module Contrôle de l'intégrité enverra également à cette adresse les notifications relatives à cet hôte précis.

- **Alarme jaune d'UC :** saisissez le seuil à partir duquel une alarme jaune doit être générée. Cette valeur correspond à la charge moyenne de l'UC. La valeur par défaut est 3 et la valeur maximale recommandée est 7.
- **Alarme rouge d'UC :** saisissez le seuil à partir duquel une alarme rouge doit être générée. Cette valeur correspond à la charge moyenne de l'UC. La valeur par défaut est 6 et la valeur maximale recommandée est 15.

- **Alarme jaune de disque :** saisissez le seuil à partir duquel une alarme jaune doit être générée. Cette valeur correspond au pourcentage d'utilisation de l'unité de disque dur. La valeur par défaut est 80 et la valeur maximale recommandée est 90.

  Une valeur de 80, par exemple, signifie qu'une alarme jaune est générée lorsque 80 % de la capacité de l'unité de disque dur est utilisée.

- **Alarme rouge de disque :** saisissez le seuil à partir duquel une alarme rouge doit être générée. Cette valeur correspond au pourcentage d'utilisation de l'unité de disque dur. La valeur par défaut est 90 et la valeur maximale recommandée est 95.

  Une valeur de 90, par exemple, signifie qu'une alarme rouge est générée lorsque 90 % de la capacité de l'unité de disque dur est utilisée.

- **Alarme jaune de mémoire :** saisissez le seuil à partir duquel une alarme jaune doit être générée. Cette valeur correspond au pourcentage de mémoire utilisée. La valeur par défaut est 50 et la valeur maximale recommandée est 75.

  Une valeur de 50, par exemple, signifie qu'une alarme jaune est générée lorsque 50 % de la mémoire est utilisée.

- **Alarme rouge de mémoire :** saisissez le seuil à partir duquel une alarme rouge doit être générée. Cette valeur correspond au pourcentage de mémoire utilisée. La valeur par défaut est 75 et la valeur maximale recommandée est 90.

  Une valeur de 75, par exemple, signifie qu'une alarme rouge est générée lorsque 75 % de la mémoire est utilisée.

Configuration des paramètres de contrôle d'intégrité

Pour configurer les paramètres du module Contrôle de l'intégrité :

1. **Sélectionnez Contrôle de l'intégrité → Paramètres.**

   Le tableau Propriétés du contrôle de l'intégrité s'affiche (voir FIGURE 4).

FIGURE 4 Tableau Propriétés du contrôle de l'intégrité

2. **Configurez les paramètres.**

   Pour consulter la liste des paramètres modifiables, reportez-vous à la section “Paramètres de contrôle d'intégrité configurables” on page 12.

3. **Cliquez sur Enregistrer.**

   Le tableau Propriétés du contrôle de l'intégrité s'actualise.

Planification d'une requête de vérification d'activité

Pour planifier une nouvelle requête de vérification d'activité :

1. **Sélectionnez Contrôle de l'intégrité → Paramètres.**

   Le tableau Propriétés du contrôle de l'intégrité s'affiche.

2. **Cliquez sur Planifier une nouvelle requête de vérification d'activité.**

   Ce bouton est situé au-dessus du tableau. Le tableau Paramètres de planification de la requête de vérification d'activité s'affiche.

3. **Configurez les paramètres.**

   Pour consulter la liste des paramètres de requête d'activité, reportez-vous à la section “Paramètres des requêtes de statut et d'activité” on page 12.

4. **Cliquez sur Enregistrer ou sur Annuler.**
   - *Si vous cliquez sur Annuler*, la tâche planifiée n'est pas enregistrée. Le tableau Tâches planifiées s'affiche, mais il ne contient pas la tâche que vous venez d'annuler.
   - *Si vous cliquez sur Enregistrer*, la tâche planifiée est ajoutée à la liste des tâches planifiées. Le tableau Tâches planifiées s'affiche ; il contient la nouvelle tâche.
5. **Ce tableau affiche les détails des tâches planifiées et permet de les modifier ou de les supprimer.**
   - Pour afficher les détails d'une tâche planifiée, cliquez sur l'icône en forme de *loupe*.
   - Pour modifier une tâche planifiée, cliquez sur l'icône en forme de *crayon*.
   - Pour supprimer une tâche planifiée, cliquez sur l'icône de *suppression*.

Planification d'une requête sur le statut

Pour planifier une nouvelle requête sur le statut :

1. **Sélectionnez Contrôle de l'intégrité → Paramètres.**

   Le tableau Propriétés du contrôle de l'intégrité s'affiche.
2. **Cliquez sur Planifier une nouvelle requête sur le statut.**

   Ce bouton est situé au-dessus du tableau. Le tableau Paramètres de planification de la requête sur le statut s'affiche.
3. **Configurez les paramètres.**

   Pour consulter la liste des paramètres modifiables, reportez-vous à la section “Paramètres des requêtes de statut et d'activité” on page 12.
4. **Cliquez sur Enregistrer ou sur Annuler.**
   - *Si vous cliquez sur Annuler*, la tâche planifiée n'est pas enregistrée. Le tableau Tâches planifiées s'affiche, mais il ne contient pas la tâche que vous venez d'annuler.
   - *Si vous cliquez sur Enregistrer*, la tâche planifiée est ajoutée à la liste des tâches planifiées. Le tableau Tâches planifiées s'affiche ; il contient la nouvelle tâche.
5. **Ce tableau affiche les détails des tâches planifiées et permet de les modifier ou de les supprimer.**

Ajout de nouveaux services au module Contrôle de l'intégrité

Le module Contrôle de l'intégrité permet d'incorporer des scripts personnalisés, de les exécuter et de les contrôler. Un script est exécuté et peut, selon les résultats obtenus, envoyer un événement entraînant une alarme ou un événement critique sur Sun Control Station. Les informations spécifiques associées à l'événement sont présentées dans le tableau Autres services de l'écran détaillé. L'effacement du contenu du tableau Événements critiques entraîne la remise à zéro des alarmes.

Afin de simplifier sa personnalisation, le module Contrôle de l'intégrité utilise un fichier de configuration servant à spécifier les détails des scripts personnalisés. Le démon de contrôle de l'intégrité extrait de ce fichier le nom du contrôle, la description, le programme à exécuter et le texte de chaque état que fournira le programme.

Les quatre états 0, 1, 2 et 3 correspondent à la gravité du problème et par conséquent à la couleur et à l'icône représentant l'état dans les tableaux de contrôle de l'intégrité. Ces états sont définis comme suit :

- État 0 = service non disponible (ligne pointillée sur cercle gris).
- État 1 = le service fonctionne normalement (coche sur cercle vert).
- État 2 = avertissement (point d'exclamation sur cercle jaune).
- État 3 = état critique (croix sur cercle rouge).

Format du fichier de configuration

Le format du fichier de configuration est le suivant :

- **version :** version du fichier de configuration ou du script de contrôle.

  Exemple : version 1.0

- **program :** chemin d'accès complet au script à exécuter à chaque intervalle.

  Exemple : `/usr/mgmt/bin/cobalt_db.pl`

- **vendor :** chaîne spécifiant le fournisseur ou le propriétaire du système de contrôle.

  Exemple : Vendor Test

- **interval :** intervalle auquel le contrôle s'exécute, exprimé en minutes.

  Exemple : 10

- **name :** chaîne indiquant le nom du contrôle.

  Exemple : Database Check

- **description :** chaîne décrivant brièvement le contrôle.

  Exemple : Monitors the database

- **state0msg :** chaîne spécifiant le message à envoyer avec un événement lorsque l'état est "non disponible" (cercle gris).

  Exemple : The database server is not monitored/state unavailable.

- **state1msg :** chaîne spécifiant le message à envoyer avec un événement lorsque l'état est "normal" (cercle vert).

  Exemple : The database server is online.

- **state2msg :** chaîne spécifiant le message à envoyer avec un événement lorsque l'état est "avertissement" (cercle jaune).

  Exemple : The database server is in limbo.

- **state3msg :** chaîne spécifiant le message à envoyer avec un événement lorsque l'état est "critique" (cercle rouge).

  Exemple : The database server is offline.

Le programme spécifié dans le fichier de configuration est requis pour le renvoi des valeurs numériques 0, 1, 2 et 3. Lorsque le démon de contrôle de l'intégrité exécute une requête (environ toutes les 10 minutes), le programme spécifié dans le fichier de configuration est exécuté.

Les résultats (0, 1, 2 ou 3) sont capturés et stockés après la première exécution du programme. Dès lors, chaque fois que le démon de contrôle de l'intégrité s'exécute, les nouveaux résultats obtenus sont comparés aux résultats précédents. S'ils diffèrent, un événement est généré, puis envoyé à la station de contrôle. Cet événement spécifie l'état et le message associé à l'état, ainsi que le nom, la version et la description du service. Si un état jaune ou rouge est renvoyé, un événement critique est généré sur la station de contrôle et une alerte de statut s'affiche dans l'angle supérieur gauche de l'interface utilisateur.

Vous devez placer le fichier de configuration dans le répertoire `/usr/mgmt/etc/hmd` et le script de contrôle dans le répertoire `/usr/mgmt/bin`.

Incluez ces étapes dans le script d'installation afin de placer les fichiers dans les répertoires appropriés lors de l'installation et de redémarrer le démon.

Création d'un nouveau service de contrôle de l'intégrité

Pour créer un nouveau service de contrôle de l'intégrité :

1. **Créez le fichier de configuration avec les différents paramètres pour le nouveau service.**

   Attribuez un *nom_de_fichier*`.conf` au fichier de configuration (par exemple `monitor_db.conf`). Tous les fichiers de configuration sont placés dans le répertoire `/usr/mgmt/etc/hmd`.

   Voici un exemple de fichier de configuration :

```
version 1.0
program /usr/mgmt/bin/monitor_db.pl
vendor Sun
interval 10
name Database
description Monitors the database.
state0msg The database server is not monitored/state unavailable.
state1msg The database server is running.
state2msg The database server is in limbo.
state3msg The database server is not running.
```

2. **Créez un script permettant de contrôler le nouveau service (le paramètre *program* du fichier de configuration).**

   Tous ces scripts de contrôle sont placés dans le répertoire `/usr/mgmt/bin`.

   Voici un exemple de script de contrôle pour le service Database Check (`monitor_db.pl`) :

```
#!/usr/bin/perl -w
# This script return whether mysql db is running
#
# return values:
#   Disabled/No info: 0
#   Running:          1
#   Not Running:      3
use strict;
use lib '/scs/lib/perl5';
use SysCmd;
```

```
if (system("/bin/ps -ef | /bin/grep mysqld | /bin/grep -v grep"))
{
   exit(3);
}
else {
   exit(1);
}
```

3. **Incluez la directive suivante dans le script d'installation pour le nouveau service de contrôle de l'intégrité.**

   Copiez le fichier de configuration et le script de contrôle dans les emplacements appropriés.

   ```
   echo "Copying script to /usr/mgmt/bin " >> $LOG
   cp /Votre_répertoire/patches/monitor_db.pl /usr/mgmt/bin/
   echo "Copying config file to /usr/mgmt/etc/hmd " >> $LOG
   cp /Votre_répertoire /patches/monitor_db.conf /usr/mgmt/etc/hmd/
   ```

4. **Créez un fichier de package pour chaque type d'hôte sur lequel vous souhaitez installer le nouveau service de contrôle de l'intégrité.**

5. **Téléchargez le package vers la station de contrôle via le module d'installation du logiciel. Utilisez le module d'installation du logiciel pour publier le package ou pour l'installer sur les hôtes sélectionnés.**

   Pour plus d'informations, reportez-vous au manuel *Sun Control Station 2.2 – Module d'installation du logiciel*.