Sun Control Station

Module Contrôle de l'intégrité

Sun Microsystems, Inc.
www.sun.com

Référence : 817-5862-10
Avril 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 d'intégrité des hôtes gérés en fonction de plusieurs paramètres. Ce document présente les fonctions et services disponibles dans ce module.

Ce module permet :

- d'afficher un récapitulatif des données du statut d'intégrité d'un hôte ou d'un groupe d'hôtes ;
- d'extraire les données de statut d'intégrité les plus récentes à partir des hôtes gérés ;
- de vérifier que vous pouvez atteindre l'agent sur un hôte géré spécifique et que cet hôte est accessible sur le réseau ;
- d'obliger la station de contrôle à extraire immédiatement les données de statut d'intégrité les plus récentes d'un hôte individuel ;
- de configurer les paramètres pour le module Contrôle de l'intégrité ;
- de saisir une adresse e-mail à laquelle seront envoyées les alertes depuis le module Contrôle de l'intégrité, lors de la génération d'événements système critiques (représentés par un cercle jaune avec un point d'exclamation ou un cercle rouge avec une croix).

Remarque : dans la plupart des procédures brèves décrites dans ce chapitre, la première étape consiste à cliquer sur l'onglet de l'élément Contrôle de l'intégrité dans la barre de menus de gauche et la deuxième à cliquer sur une option du sous-menu.

Pour réduire le nombre d'étapes de chaque procédure, les commandes de menu sont regroupées et affichées avec une majuscule au début du premier mot. Un signe "supérieur à" (>) sépare chaque élément.

La formule "Sélectionnez Contrôle de l'intégrité > Afficher les hôtes", par exemple, signifie que devez cliquer sur Contrôle de l'intégrité dans la barre de menus de gauche, puis cliquer sur l'option de sous-menu Afficher les hôtes.

Modèle de contrôle

Le modèle mis en place pour le module Contrôle de l'intégrité est basé sur des requêtes et des événements. Cela signifie que les données de statut d'intégrité sont acquises par la station de contrôle qui initie un intervalle de requête pour la lecture des informations relatives à l'état du client pour chaque hôte ou par l'hôte géré informant la station de contrôle de la présence d'un problème (*événement*).

Le modèle d'événement permet d'être informé instantanément en cas de problème.

La FIGURE 1 offre un exemple des tableaux Événements critiques et Statut du groupe d'hôtes gérés.

FIGURE 1 Tableaux de contrôle de l'intégrité

Couleurs de statut

Le statut de chaque service ou composant matériel est signalé par un cercle de couleur et une icône (gris avec des points de suspension, vert avec une coche, jaune avec un point d'exclamation ou rouge avec une croix) en regard de chaque élément. Les couleurs ont la signification suivante :

Gris avec des points de suspension : indique qu'aucune information n'est disponible ou que le service ou la fonction de contrôle ne sont pas activés sur l'hôte.

Vert avec une coche : indique que le service ou le composant fonctionnent normalement.

Jaune avec un point d'exclamation : indique que l'utilisation sur l'hôte est modérée ou qu'un composant est en cours de récupération.

Rouge avec une croix : indique que l'utilisation sur l'hôte est importante ou qu'une erreur s'est produite.

Alerte de contrôle de l'intégrité

Si un événement de type 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 lorsqu'un événement se transforme en avertissement ou en événement critique, c'est-à-dire lorsque l'état jaune ou rouge est renvoyé lors de la requête d'intégrité.

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

Problèmes connus

Paramètres conflictuels

Il est possible de gérer un hôte à l'aide de plusieurs stations Sun Control Station. Vous pouvez modifier les paramètres de contrôle de l'intégrité (notamment les seuils d'alarme d'UC) depuis n'importe quelle station de contrôle : lors de la modification des paramètres sur une station de contrôle, les nouvelles valeurs sont transmises à tous les hôtes gérés.

Les valeurs des tout derniers paramètres modifiés remplacent alors les valeurs précédentes de l'hôte géré. Les paramètres qui apparaissent dans les interfaces utilisateur des autres stations de contrôle ne sont toutefois pas mis à jour et ne reflètent pas les modifications de paramètres les plus récentes.

Pour résoudre ce problème, si plus d'une station de contrôle gère un ou plusieurs hôtes spécifiques, assurez-vous que les paramètres de contrôle de l'intégrité sont identiques sur chacune de ces stations de contrôle.

Informations inattendues sur la gestion en service réduit lors du contrôle de l'intégrité

Vous pouvez gérer un hôte depuis deux stations de contrôle différentes.

Dans ce cas particulier :

- le module de contrôle Gestion en service réduit est installé sur l'une des stations de contrôle, mais pas sur l'autre ;
- côté client, les bits du module de contrôle Gestion en service réduit ont été installés sur l'hôte géré.

L'hôte géré est à présent activé de manière à fournir les informations sur la gestion en service réduit à la première station de contrôle. Ces informations s'affichent dans les tableaux de contrôle de l'intégrité.

Le module Contrôle de l'intégrité étant toutefois conçu pour recevoir les informations sur la gestion en service réduit lorsqu'elles sont disponibles, les tableaux de contrôle de l'intégrité de la deuxième station de contrôle afficheront également ces informations, même si le module Contrôle de la gestion en service réduit n'a pas été installé sur cette deuxième station de contrôle.

Il ne s'agit pas d'un bogue ni d'une défaillance sur la deuxième station de contrôle, mais juste d'une indication pour vous signaler que vous pouvez également afficher les informations sur la gestion en service réduit dans les tableaux de contrôle de l'intégrité.

Écran Contrôle de l'intégrité

Pour afficher le statut actuel des services et des composants matériels des hôtes gérés ou le mettre à jour, cliquez sur l'option de menu Contrôle de l'intégrité sur la gauche, 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, page 5)
- Afficher les hôtes (voir Affichage des hôtes, page 10)
- Paramètres (voir Paramètres, page 12)

Récapitulatif de l'intégrité

L'option de sous-menu Récapitulatif 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. Pour plus d'informations, reportez-vous à la FIGURE 1.

- Le tableau Événements critiques affiche les événements que l'administrateur devrait envoyer immédiatement.
- Le tableau Statut du groupe d'hôtes gérés affiche le statut général des groupes d'hôtes présents 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 les 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 d'exécution sur cet hôte spécifique, par exemple sur le serveur FTP, Telnet, DNS ou sur le serveur d'e-mail (ces éléments peuvent varier selon le type d'hôte affiché) ;
- Le tableau Autres services système qui affiche les informations sur les services de tiers ou 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, page 17.

Affichage des données de contrôle de l'intégrité

Pour afficher un récapitulatif des données de contrôle de l'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 sur l'icône en forme de *loupe* située en regard de l'élément dans la colonne Actions.**

   Les tableaux informatifs s'affichent. Pour plus d'informations, reportez-vous à la FIGURE 2.

   - Composants système principaux
   - Services principaux
   - Autres services système

   Pour revenir à l'écran précédent, cliquez sur l'icône en forme de *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 et répertorie les hôtes appartenant à ce groupe.**

   Vous pouvez cliquer sur l'icône en forme de *loupe* située en regard de l'hôte dans la colonne Actions. Cette opération entraîne l'affichage des trois tableaux informatifs mentionnés ci-dessus.

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

FIGURE 2 Tableaux informatifs détaillés

Actualisation de l'interface utilisateur

Un bouton Actualiser est situé au-dessus du tableau Événements critiques. Il permet de mettre instantanément à jour le cadre de l'interface utilisateur, de manière à ce que ce dernier reflète les données les plus récentes figurant dans 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 figurant dans la base de données, reportez-vous à la section Mise à jour des données de statut d'intégrité, page 9.

Services contrôlés sur des serveurs Sun Cobalt

Les services contrôlés sur des serveurs Sun Cobalt peuvent comprendre :

Remarque : certains de ces services ne sont pas disponibles sur tous les types de serveurs Sun Cobalt.

- Active Server Pages (ASP)
- Appleshare
- Protection contre le dépassement de la capacité du buffer
- Serveur DHCP
- Serveur DNS
- Serveurs d'e-mail (POP/IMAP/SMTP)
- Serveur FTP
- JavaServer Pages™ (JSP™) et servlets
- Détection de scanner
- Server Desktop
- Serveur SNMP
- Serveur Telnet
- Serveur Web
- Serveur de partage de fichiers Windows

Services contrôlés sur des hôtes autres que des serveurs

Les services contrôlés sur des hôtes autres que des serveurs comprennent :

- Serveur DNS
- Serveur d'e-mail
- Serveur FTP
- Serveur MySQL
- Serveur SSH
- Serveur Telnet
- Serveur Web

Effacement d'un ou de plusieurs événements critiques

Les événements critiques générés sur un hôte géré s'affichent dans le tableau Événements critiques. Si vous choisissez de ne pas traiter un événement critique spécifique, vous pouvez l'effacer du tableau. Cette opération ne supprime pas le problème de l'hôte géré, mais elle garantit que vous ne recevrez plus de notification relative à cet événement critique 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 événement critique spécifique 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 du tableau un événement critique spécifique, cliquez sur l'icône de *suppression* située en regard de l'événement dans la colonne Actions.**

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

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

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

Mise à jour des données de statut d'intégrité

Vous pouvez mettre à jour les données de statut d'intégrité pour chaque hôte. Grâce à cette fonction, la station de contrôle extrait instantanément d'un hôte les données de statut d'intégrité les plus récentes.

Le bouton Mettre à jour maintenant s'affiche dans l'interface utilisateur lorsque vous affichez les tableaux informatifs 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 sur l'icône en forme de *loupe* située en regard de l'élément dans la colonne Actions.**

   Les tableaux informatifs détaillés s'affichent.

3. **Si vous visualisez les détails d'un événement critique, les tableaux informatifs 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.**

   Vous pouvez cliquer sur l'icône en forme de *loupe* située en regard de l'hôte dans la colonne Actions. Cette opération entraîne l'affichage des trois tableaux informatifs mentionnés ci-dessus.
5. **Dans l'écran affichant les tableaux informatifs détaillés pour l'hôte, cliquez sur Mettre à jour maintenant au-dessus du tableau.**

   Cette opération oblige 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 ou aux écrans précédents, cliquez sur l'icône en forme de *flèche vers le haut* dans l'angle supérieur droit.**

Affichage des 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 une liste des hôtes gérés. Pour plus d'informations, reportez-vous à la FIGURE 3.

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

---

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

   Les tableaux informatifs suivants s'affichent :
   - Composants système principaux
   - Services principaux
   - Autres services système

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

3. **Dans l'écran affichant les tableaux informatifs détaillés pour l'hôte, vous pouvez cliquer sur Mettre à jour maintenant au-dessus du tableau.**

   Cette opération oblige 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 ou aux écrans précédents, cliquez sur l'icône en forme de *flèche vers le haut* dans l'angle supérieur droit.**

FIGURE 3 Tableau État des hôtes gérés

Actualisation de l'interface utilisateur

Un bouton Actualiser est situé au-dessus du tableau État des hôtes gérés. Il permet de mettre instantanément à jour le cadre de l'interface utilisateur, de manière à ce que ce dernier reflète les données les plus récentes figurant dans 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 exemple de la FIGURE 2).

2. Une commande ping est envoyée à l'hôte pour lequel l'agent a "échoué", via le protocole ICMP (Internet Control Message Protocol) afin de vérifier la connexion réseau.

   Si ce ping ICMP est fructueux, le tableau informatif du 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 en cas de défaillance de l'agent SCS), la durée d'interrogation de cet hôte est limitée à dix (10) minutes.

Si la station de contrôle détecte plusieurs hôtes inaccessibles pendant un cycle d'interrogation, un cycle spécifique peut ne terminer qu'au début du cycle d'interrogation suivant.

L'intervalle de requête sur le statut est d'une heure. Si Sun Control Station gère plusieurs hôtes, il est préférable de définir un intervalle plus long.

Configuration des paramètres

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. Pour plus d'informations, reportez-vous à la FIGURE 4.

2. **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 sont envoyées les alertes depuis le module Contrôle de l'intégrité lorsque des événements système critiques sont détectés (cercle rouge).

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

Remarque : si, lorsque vous ajoutez un hôte à la station de contrôle, vous saisissez une adresse e-mail pour l'administrateur de ce hôte, les notifications pour cet hôte spécifique seront envoyées à cette adresse depuis le module Contrôle de l'intégrité.

- Alarme jaune d'UC : saisissez le seuil à partir duquel une alarme jaune doit être générée. Cette valeur correspond au chargement moyen 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 au chargement moyen 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 du lecteur 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 du lecteur 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 du lecteur 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 du lecteur 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.

3. **Cliquez sur Enregistrer.**

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

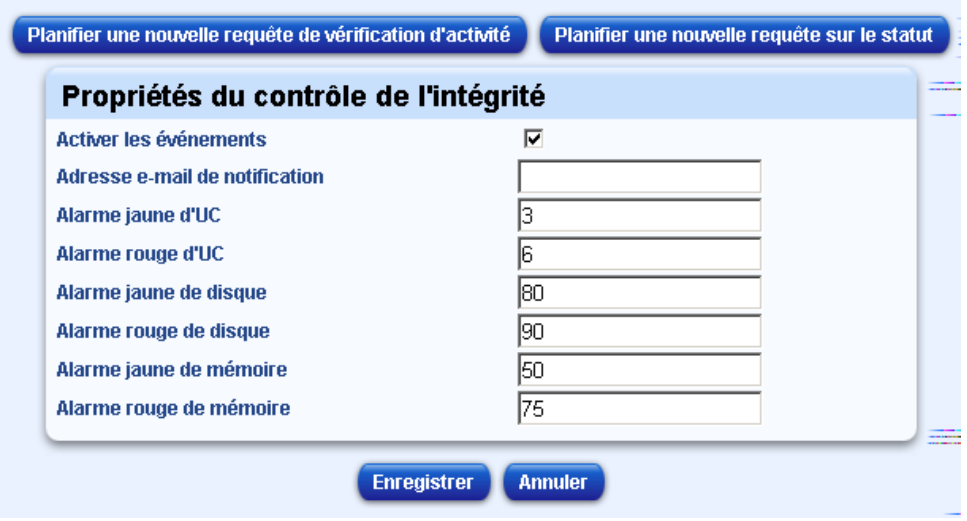

FIGURE 4 Tableau Propriétés du contrôle de l'intégrité

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 au-dessus du tableau.**

   Le tableau Paramètres de planification de la requête de vérification d'activité s'affiche. Configurez les paramètres suivants :

   - Intervalle d'exécution : définissez l'intervalle auquel la station de contrôle doit effectuer une tentative de communication avec les hôtes gérés, par exemple toutes les six (6) heures.
   - Minute(s) d'exécution : sélectionnez la ou les minutes de l'heure auxquelles vous souhaitez exécuter la requête de vérification d'activité. Mettez en évidence les minutes et utilisez les touches fléchées pour les déplacer d'une liste déroulante à l'autre.
   - Adresse e-mail (facultative) : 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.

3. **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 et contient la nouvelle tâche.

4. **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 au-dessus du tableau.**

   Le tableau Paramètres de planification de la requête sur le statut s'affiche. Configurez les paramètres suivants :

   - Intervalle d'exécution : définissez l'intervalle auquel la station de contrôle doit solliciter les données d'intégrité aux hôtes gérés, par exemple toutes les six (6) heures.
   - Minute(s) d'exécution : sélectionnez la ou les minutes de l'heure auxquelles vous souhaitez exécuter la requête sur le statut. Mettez en évidence les minutes et utilisez les touches fléchées pour les déplacer d'une liste déroulante à l'autre.
   - Adresse e-mail (facultative) : saisissez l'adresse e-mail de la personne qui sera notifiée de l'exécution de la requête sur le statut.
   - 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.

3. **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 et contient la nouvelle tâche.

4. **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 à exécuter et à 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 informatif détaillé. L'effacement du contenu du tableau Événements critiques entraîne la remise à zéro des alarmes.

Pour faciliter la personnalisation du module Contrôle de l'intégrité, ce dernier utilise un fichier de configuration pour la spécification des détails des scripts personnalisés. Depuis ce fichier, le démon de contrôle de l'intégrité acquiert le nom du contrôle, la description, le programme à exécuter et le texte de chaque état que fournira le programme.

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

- État 0 = Service non disponible (gris avec des points de suspension)
- État 1 = Le service fonctionne normalement (vert avec une coche)
- État 2 = Avertissement (jaune avec un point d'exclamation)
- État 3 = État critique (rouge avec une croix)

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 qui spécifie le fournisseur ou le propriétaire du système de contrôle

  Exemple : Test fournisseur

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

  Exemple : 10

- name : chaîne indiquant le nom du contrôle

  Exemple : Contrôle de la base de données

- description : chaîne spécifiant une description brève du contrôle

  Exemple : Contrôle la base de données

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

  Exemple : Le serveur de base de données n'est pas contrôlé ou l'état n'est pas disponible.

- state1msg : chaîne spécifiant le message à envoyer avec un événement lorsque l'état est de type fonctionnement correct (cercle vert)

  Exemple : Le serveur de base de données est en ligne.

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

  Exemple : Le serveur de base de données ne répond pas.

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

  Exemple : Le serveur de base de données est hors ligne.

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 valide (environ toutes les 10 minutes), le programme spécifié dans le fichier de configuration s'exécute.

Les résultats (0, 1, 2 ou 3) sont capturés et stockés après la première exécution du programme. Dès lors, les résultats sont comparés aux résultats précédents à chaque exécution du démon de contrôle de l'intégrité. 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

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 au fichier de configuration `filename.conf` (par exemple `cobalt_db.conf`). Tous les fichiers de configuration sont placés dans le répertoire `/usr/mgmt/etc/hmd`.

   L'apparence d'un fichier de configuration peut être la suivante :

```
version 1.0
program /usr/mgmt/bin/cobalt_cpu.pl
detail :81/cgi-bin/.cobalt/cpuUsage/cpuUsage.cgi
vendor Sun
interval 10
name CPU
description Cobalt CPU Monitor
state0msg The CPU is not monitored/state unavailable.
state1msg The CPU is lightly used.
state2msg The CPU is moderately used.
state3msg The CPU is heavily used.
yellowalarm 3
redalarm 6
alarmtitle load of the CPU
```

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, par exemple, l'apparence du script de contrôle pour le service Contrôle de la base de données (`cobalt_db.pl`) :

```
#!/usr/bin/perl
use strict;

# cobalt_cpu.pl - health monitoring script for the CPU
#
# Details:
#
# This script is used in conjunction with the health monitoring daemon
(hmd)
# for use with "Big Daddy".IPC is accomplished by setting the proper
exit
# code of this script. The following exit codes coincide with the
following
# states:
#
# -1 - fatal error
# 0  - n/a    ( unmonitored/state unavailable )
# 1  - green  ( normal state )
# 2  - yellow ( warning state )
# 3  - red    ( critical state )
#
# Based up the exit code, the hmd will react by sending an event to the
# management station with the information defined in the config file
for
# this service.

my $yel_thresh = $ARGV[0] || 3;
my $red_thresh = $ARGV[1] || 6;
my $fifteen;
```

```
open(LOAD,"/proc/loadavg") or out(-1);
my $line = <LOAD>;
$line =~ /^(\d+\.\d+)\s*(\d+\.\d+)\s*(\d+\.\d+)/o;
close LOAD;
$fifteen = $3;

if ($fifteen >= $red_thresh) {
                  exit 3;
} elsif ($fifteen >= $yel_thresh ) {
                  exit 2;
} 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 /YourDirectory/patches/cobalt_db.pl /usr/mgmt/bin/
   echo "Copying config file to /usr/mgmt/etc/hmd " >> $LOG
   cp /YourDirectory /patches/cobalt_db.conf /usr/mgmt/etc/hmd/
   ```

4. **Créez un fichier de package pour chaque type d'hôte sur lequel vous souhaitez installer ce nouveau service de contrôle de l'intégrité (par exemple, un serveur Sun LX50 ou un Sun Cobalt Qube™ 3).**

5. **Téléchargez le package vers la station de contrôle via le module Gestion des logiciels. Utilisez le module Gestion des logiciels pour publier le package ou pour l'installer sur les hôtes sélectionnés.**

   Pour plus d'informations, reportez-vous au document PDF *Module Gestion des logiciels*.