Modifier le nom d'hôte d'Unified Manager

Active IQ Unified Manager

NetApp
January 15, 2026

Sommaire

Modifier le nom d’hôte d’Unified Manager

Il peut être nécessaire de modifier le nom d’hôte du système sur lequel vous avez installé Unified Manager. Par exemple, vous pouvez renommer l’hôte pour identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de clusters surveillé.

Les étapes requises pour modifier le nom d’hôte sont différentes selon que Unified Manager s’exécute sur un serveur VMware ESXi, sur un serveur Red Hat Linux ou sur un serveur Microsoft Windows.

Modifier le nom d’hôte de l’appliance virtuelle Unified Manager

Un nom est attribué à l’hôte réseau lors du premier déploiement de l’appliance virtuelle Unified Manager. Vous pouvez modifier le nom d’hôte après le déploiement. Si vous modifiez le nom d’hôte, vous devez également régénérer le certificat HTTPS.

Avant de commencer

Vous devez être connecté à Unified Manager en tant qu’utilisateur de maintenance, ou avoir le rôle d’administrateur d’applications qui vous est attribué pour effectuer ces tâches.

Vous pouvez utiliser le nom d’hôte (ou l’adresse IP de l’hôte) pour accéder à l’interface utilisateur Web Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau pendant le déploiement, vous avez alors désigné un nom pour l’hôte réseau. Si vous avez configuré le réseau à l’aide de DHCP, le nom d’hôte doit être pris du DNS. Si DHCP ou DNS n’est pas correctement configuré, le nom d’hôte « Unified Manager » est automatiquement attribué et associé au certificat de sécurité.

Quel que soit le mode d’attribution du nom d’hôte, si vous modifiez le nom d’hôte et que vous prévoyez d’utiliser le nouveau nom d’hôte pour accéder à l’interface utilisateur Web Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l’interface utilisateur Web à l’aide de l’adresse IP du serveur au lieu du nom d’hôte, vous n’avez pas à générer de nouveau certificat si vous modifiez le nom d’hôte. Toutefois, il est recommandé de mettre à jour le certificat de sorte que le nom d’hôte du certificat corresponde au nom d’hôte réel.

Si vous modifiez le nom d’hôte dans Unified Manager, vous devez mettre à jour manuellement le nom d’hôte dans OnCommand Workflow Automation (WFA). Le nom d’hôte n’est pas mis à jour automatiquement dans WFA.

Le nouveau certificat n’est effectif qu’après le redémarrage de la machine virtuelle Unified Manager.

Étapes

1. Générez un certificat de sécurité HTTPS

   Si vous souhaitez utiliser le nouveau nom d’hôte pour accéder à l’interface utilisateur Web d’Unified Manager, vous devez régénérer le certificat HTTPS pour l’associer au nouveau nom d’hôte.

2. Redémarrez la machine virtuelle Unified Manager

   Après la régénération du certificat HTTPS, vous devez redémarrer la machine virtuelle Unified Manager.

Générer un certificat de sécurité HTTPS

Lors de la première installation de Active IQ Unified Manager, un certificat HTTPS par défaut est installé. Vous pouvez générer un nouveau certificat de sécurité HTTPS qui remplace le certificat existant.

Avant de commencer

Vous devez avoir le rôle Administrateur d'applications.

Il peut y avoir plusieurs raisons de régénérer le certificat, par exemple si vous souhaitez avoir de meilleures valeurs pour le nom unique (DN) ou si vous voulez une taille de clé plus élevée, ou une période d'expiration plus longue ou si le certificat actuel a expiré.

Si vous n'avez pas accès à l'interface utilisateur Web d'Unified Manager, vous pouvez régénérer le certificat HTTPS avec les mêmes valeurs à l'aide de la console de maintenance. Pendant la régénération des certificats, vous pouvez définir la taille de la clé et la durée de validité de la clé. Si vous utilisez le `Reset Server Certificate` Disponible sur la console de maintenance, un nouveau certificat HTTPS est créé pendant 397 jours. Ce certificat sera doté d'une clé RSA de taille 2048 bits.

Étapes

1. Dans le volet de navigation de gauche, cliquez sur **général** > **certificat HTTPS**.
2. Cliquez sur **régénérer le certificat HTTPS**.

   La boîte de dialogue régénérer le certificat HTTPS s'affiche.

3. Sélectionnez l'une des options suivantes en fonction de la façon dont vous souhaitez générer le certificat :

Les fonctions que vous recherchez…	Procédez comme ça…
Régénérer le certificat avec les valeurs actuelles	Cliquez sur l'option **régénérer en utilisant les attributs de certificat actuels**.

Les fonctions que vous recherchez…	Procédez comme ça…
Générez le certificat à l'aide de valeurs différentes	Cliquez sur l'option **mettre à jour les attributs de certificat actuels**. Les champs Nom commun et noms alternatifs utiliseront les valeurs du certificat existant si vous ne saisissez pas de nouvelles valeurs. Le « Nom commun » doit être défini sur le FQDN de l'hôte. Les autres champs ne nécessitent pas de valeurs, mais vous pouvez entrer des valeurs, par exemple pour l'E-MAIL, LA SOCIÉTÉ, LE SERVICE, Ville, État et pays si vous souhaitez que ces valeurs soient renseignées dans le certificat. Vous pouvez également sélectionner la TAILLE DE CLÉ disponible (l'algorithme clé est « RSA ») et LA PÉRIODE DE VALIDITÉ. • Les valeurs autorisées pour la taille de clé sont `2048`, `3072` et `4096`. • Les périodes de validité sont de 1 jour minimum à 36500 jours maximum. Même si une période de validité de 36500 jours est autorisée, il est recommandé d'utiliser une période de validité d'au plus 397 jours ou 13 mois. Puisque si vous sélectionnez une période de validité de plus de 397 jours et que vous prévoyez d'exporter une RSC pour ce certificat et de l'obtenir signé par une CA connue, la validité du certificat signé vous sera réduite à 397 jours. • Vous pouvez cocher la case « exclure les informations d'identification locales (par exemple localhost) » si vous souhaitez supprimer les informations d'identification locales du champ autres noms du certificat. Lorsque cette case est cochée, seul ce que vous saisissez dans le champ est utilisé dans le champ autres noms. Si le champ du certificat obtenu n'est pas renseigné, il n'y aura pas de champ autre nom.

4. Cliquez sur **Oui** pour régénérer le certificat.
5. Redémarrez le serveur Unified Manager afin que le nouveau certificat prenne effet.
6. Vérifiez les nouvelles informations de certificat en consultant le certificat HTTPS.

Redémarrez la machine virtuelle Unified Manager

Vous pouvez redémarrer le serveur virtuel à partir de la console de maintenance d'Unified Manager. Vous devez redémarrer après avoir généré un nouveau certificat de sécurité ou en cas de problème avec la machine virtuelle.

Avant de commencer

L'appliance virtuelle est sous tension.

En tant qu'utilisateur de maintenance, vous êtes connecté à la console de maintenance.

Vous pouvez également redémarrer la machine virtuelle depuis vSphere en utilisant l'option **redémarrer invité**. Pour plus d'informations, consultez la documentation VMware.

Étapes

1. Accéder à la console de maintenance.
2. Sélectionnez **Configuration du système** > **redémarrer la machine virtuelle**.

Modifier le nom d'hôte d'Unified Manager sur les systèmes Linux

À un moment donné, vous pouvez modifier le nom d'hôte de la machine Red Hat Enterprise Linux sur laquelle vous avez installé Unified Manager. Par exemple, vous pouvez renommer l'hôte pour identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de clusters surveillé lorsque vous répertoriez vos machines Linux.

Avant de commencer

Vous devez avoir un accès utilisateur root au système Linux sur lequel Unified Manager est installé.

Vous pouvez utiliser le nom d'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface utilisateur Web Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau pendant le déploiement, vous avez alors désigné un nom pour l'hôte réseau. Si vous avez configuré le réseau à l'aide de DHCP, le nom d'hôte doit être pris du serveur DNS.

Quel que soit le mode d'attribution du nom d'hôte, si vous modifiez le nom d'hôte et que vous envisagez d'utiliser le nouveau nom d'hôte pour accéder à l'interface utilisateur Web d'Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l'interface utilisateur Web à l'aide de l'adresse IP du serveur au lieu du nom d'hôte, vous n'avez pas à générer de nouveau certificat si vous modifiez le nom d'hôte. Toutefois, il est recommandé de mettre à jour le certificat, de sorte que le nom d'hôte du certificat corresponde au nom d'hôte réel. Le nouveau certificat ne prend pas effet tant que la machine Linux n'est pas redémarrée.

Si vous modifiez le nom d'hôte dans Unified Manager, vous devez mettre à jour manuellement le nom d'hôte dans OnCommand Workflow Automation (WFA). Le nom d'hôte n'est pas mis à jour automatiquement dans

WFA.

Étapes

1. Connectez-vous en tant qu'utilisateur root au système Unified Manager que vous souhaitez modifier.
2. Pour arrêter le logiciel Unified Manager et le logiciel MySQL associé, saisissez la commande suivante :

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Modifiez le nom d'hôte à l'aide de Linux `hostnamectl` commande :

   ```
   hostnamectl set-hostname new_FQDN
   ```

   ```
   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. Régénérer le certificat HTTPS pour le serveur :

   ```
   /opt/netapp/essentials/bin/cert.sh create
   ```

5. Redémarrez le service réseau :

   ```
   systemctl restart NetworkManager.service
   ```

6. Une fois le service redémarré, vérifiez si le nouveau nom d'hôte peut s'envoyer par commande ping :

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   Cette commande doit renvoyer la même adresse IP que celle définie précédemment pour le nom d'hôte d'origine.

7. Une fois que vous avez terminé et vérifié la modification de votre nom d'hôte, redémarrez Unified Manager en entrant la commande suivante :

   ```
   systemctl start mysqld ocie ocieau
   ```

Informations sur le copyright

Informations sur les marques commerciales