# Modifier le nom de l'hôte de Unified Manager

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager-918/config/task_change_unified_manager_host_name_on_vmware.html on November 13, 2026. Always check docs.netapp.com for the latest.

# Sommaire

Modifier le nom de l’hôte de Unified Manager . . . . . 1
Modifier le nom de l’hôte de l’appliance virtuelle Active IQ Unified Manager . . . . . 1
Générez un certificat de sécurité HTTPS dans Active IQ Unified Manager . . . . . 1
Redémarrez la machine virtuelle Active IQ Unified Manager . . . . . 4
Modifier le nom de l’hôte Active IQ Unified Manager sur les systèmes Linux . . . . . 4

# Modifier le nom de l'hôte de Unified Manager

## Modifier le nom de l'hôte de l'appliance virtuelle Active IQ Unified Manager

L'hôte réseau se voit attribuer un nom lors du premier déploiement de l'appliance virtuelle Unified Manager. Vous pouvez modifier le nom de l'hôte après le déploiement. Si vous modifiez le nom de l'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 disposer du rôle Application Administrator pour effectuer ces tâches.

Vous pouvez utiliser le nom de l'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface utilisateur web de Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau lors du déploiement, vous avez alors attribué un nom à l'hôte réseau. Si vous avez configuré le réseau à l'aide de DHCP, le nom de l'hôte doit être obtenu à partir du DNS. Si DHCP ou DNS n'est pas correctement configuré, le nom de l'hôte "Unified Manager" est automatiquement attribué et associé au certificat de sécurité.

Quelle que soit la manière dont le nom de l'hôte a été attribué, si vous modifiez le nom de l'hôte et que vous avez l'intention d'utiliser le nouveau nom de l'hôte pour accéder à l'interface utilisateur Web de Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l'interface web en utilisant l'adresse IP du serveur au lieu du nom de l'hôte, vous n'avez pas besoin de générer un nouveau certificat si vous modifiez le nom de l'hôte. Cependant, il est recommandé, conformément aux bonnes pratiques, de mettre à jour le certificat afin que le nom de l'hôte qui y figure corresponde au nom de l'hôte réel.

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

Le nouveau certificat ne prendra effet qu'après le redémarrage de la machine virtuelle Unified Manager.

**Étapes**

1. Générer un certificat de sécurité HTTPS

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

2. Redémarrez la machine virtuelle Unified Manager

   Après avoir régénéré le certificat HTTPS, vous devez redémarrer la machine virtuelle Unified Manager.

# Générez un certificat de sécurité HTTPS dans Active IQ Unified Manager

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 pour remplacer le certificat existant.

**Avant de commencer**

Vous devez posséder le rôle d'administrateur d'application.

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

Si vous n'avez pas accès à l'interface utilisateur web de Unified Manager, vous pouvez régénérer le certificat HTTPS avec les mêmes valeurs à l'aide de la console de maintenance. Lors de la régénération des certificats, vous pouvez définir la taille de la clé et sa durée de validité. Si vous utilisez l' `Reset Server Certificate` option de la console de maintenance, un nouveau certificat HTTPS valable pendant 397 jours est créé. Ce certificat aura une clé RSA de 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 manière dont vous souhaitez générer le certificat :

| Si vous voulez… | Faites ceci… |
| --- | --- |
| Régénérez le certificat avec les valeurs actuelles | Cliquez sur l'option **Régénérer en utilisant les attributs du certificat actuel**. |

| Si vous voulez… | Faites ceci… |
| --- | --- |
| Générez le certificat en utilisant différentes valeurs | Cliquez sur l'option **Mettre à jour les attributs du certificat actuel**.<br><br>Les champs Common Name et Alternative Names utiliseront les valeurs du certificat existant si vous ne saisissez pas de nouvelles valeurs. Le champ "Common Name" doit être défini sur le FQDN de l'hôte. Les autres champs ne nécessitent pas de valeurs, mais vous pouvez en saisir, par exemple pour EMAIL, COMPANY, DEPARTMENT, City, State et Country si vous souhaitez que ces valeurs soient renseignées dans le certificat. Vous pouvez également sélectionner parmi les options disponibles de KEY SIZE (l'algorithme de clé est "RSA".) et de VALIDITY PERIOD.<br><br>• Les valeurs autorisées pour la taille de la clé sont `2048`, `3072` et `4096`.<br>• Les périodes de validité vont de 1 jour minimum à 36500 jours maximum.<br><br>Bien qu'une période de validité de 36 500 jours soit autorisée, il est recommandé de ne pas utiliser une période de validité supérieure à 397 jours ou 13 mois. En effet, si vous choisissez une période de validité supérieure à 397 jours et prévoyez d'exporter une CSR pour ce certificat et de la faire signer par une CA reconnue, la validité du certificat signé que la CA vous renverra sera réduite à 397 jours.<br><br>• 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, seules les informations que vous saisissez dans le champ sont utilisées dans le champ « Autres noms ». Si ce champ est laissé vide, le certificat obtenu ne comportera aucun champ « Autres noms ». |

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

# Redémarrez la machine virtuelle Active IQ Unified Manager

Vous pouvez redémarrer la machine virtuelle depuis 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 allumée.

Vous êtes connecté à la console de maintenance en tant qu'utilisateur de maintenance.

Vous pouvez également redémarrer la machine virtuelle depuis vSphere à l'aide de l'option **Restart Guest**. Consultez la documentation VMware pour plus d'informations.

**Étapes**

1. Accédez à la console de maintenance.
2. Sélectionnez **Configuration système** > **Redémarrer la machine virtuelle**.

# Modifier le nom de l'hôte Active IQ Unified Manager sur les systèmes Linux

À un moment donné, vous pourriez souhaiter modifier le nom de l'hôte de la machine Red Hat Enterprise Linux sur laquelle vous avez installé Unified Manager. Par exemple, vous pourriez vouloir renommer cet hôte afin d'identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de clusters surveillés lorsque vous affichez la liste de vos machines Linux.

**Avant de commencer**

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

Vous pouvez utiliser le nom de l'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface web de Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau lors du déploiement, vous avez alors attribué un nom à l'hôte réseau. Si vous avez configuré le réseau à l'aide du protocole DHCP, le nom de l'hôte doit être récupéré auprès du serveur DNS.

Quelle que soit la manière dont le nom de l'hôte a été attribué, si vous modifiez le nom de l'hôte et avez l'intention d'utiliser le nouveau nom de l'hôte pour accéder à l'interface utilisateur Web de Unified Manager, vous devez générer un nouveau certificat de sécurité.

Si vous accédez à l'interface web en utilisant l'adresse IP du serveur au lieu du nom de l'hôte, vous n'avez pas à générer un nouveau certificat si vous modifiez le nom de l'hôte. Toutefois, il est recommandé, comme bonne pratique, de mettre à jour le certificat afin que le nom de l'hôte qui y figure corresponde au nom de l'hôte réel. Le nouveau certificat ne prend effet qu'après le redémarrage de la machine Linux.

Si vous modifiez le nom de l'hôte dans Unified Manager, vous devez mettre à jour manuellement le nom de

l'hôte dans OnCommand Workflow Automation (WFA). Le nom de l'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. Arrêtez le logiciel Unified Manager et le logiciel MySQL associé en saisissant la commande suivante :

   ```
   systemctl stop ocieau ocie mysqld
   ```

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

   ```
   hostnamectl set-hostname new_FQDN

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

4. Régénérez 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 de l'hôte peut se joindre lui-même par ping :

   ```
   ping new_hostname

   ping nuhost
   ```

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

7. Après avoir effectué et vérifié la modification du nom de l'hôte, redémarrez Unified Manager en saisissant la commande suivante :

   ```
   systemctl start mysqld ocie ocieau
   ```

## Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.