Modifier le nom d'hôte d'Unified Manager

Active IQ Unified Manager

NetApp
October 15, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager-916/config/task_generate_an_https_security_certificate_ocf.html on October 15, 2025. Always check docs.netapp.com for the latest.

Sommaire

Modifier le nom d’hôte d’Unified Manager

À un moment donné, vous souhaiterez peut-être modifier le nom d’hôte du système sur lequel vous avez installé Unified Manager. Par exemple, vous souhaiterez peut-être renommer l’hôte pour identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de cluster surveillé.

Les étapes requises pour modifier le nom d’hôte sont différentes selon qu’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 de l’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 disposer du 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 d’Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau lors du déploiement, vous auriez alors désigné un nom pour l’hôte du réseau. Si vous avez configuré le réseau à l’aide de DHCP, le nom d’hôte doit être extrait 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.

Quelle que soit la manière dont le nom d’hôte a été attribué, si vous modifiez le nom d’hôte et que vous avez l’intention 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 en utilisant l’adresse IP du serveur au lieu du nom d’hôte, vous n’avez pas besoin de générer un nouveau certificat si vous modifiez le nom d’hôte. Cependant, il est recommandé de mettre à jour le certificat afin que le nom d’hôte dans le 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 ne prend effet qu’une fois la machine virtuelle Unified Manager redémarrée.

Étapes

1. Générer 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. Redémarrer la machine virtuelle Unified Manager

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

Générer un certificat de sécurité HTTPS

Lorsque Active IQ Unified Manager est installé pour la première fois, 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 disposer du rôle d'administrateur d'application.

Il peut y avoir plusieurs raisons de régénérer le certificat, par exemple si vous souhaitez avoir de meilleures valeurs pour le nom distinctif (DN) ou si vous souhaitez 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 d'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 la durée de validité de la clé. Si vous utilisez le `Reset Server Certificate` option depuis la console de maintenance, puis un nouveau certificat HTTPS est créé qui est valable 397 jours. Ce certificat aura 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 manière dont vous souhaitez générer le certificat :

Si vous voulez…	Fais ceci…
Régénérer le certificat avec les valeurs actuelles	Cliquez sur l'option **Régénérer à l'aide des attributs de certificat actuels**.

Si vous voulez…	Fais ceci…
Générer le certificat en utilisant différentes valeurs	Cliquez sur l'option **Mettre à jour les attributs du certificat actuel**. 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 saisir des valeurs, par exemple, pour l'E-MAIL, l'ENTREPRISE, le SERVICE, la Ville, l'État et le Pays si vous souhaitez que ces valeurs soient renseignées dans le certificat. Vous pouvez également sélectionner parmi la TAILLE DE CLÉ disponible (l'algorithme de clé est « RSA ») et la PÉRIODE DE VALIDITÉ. • Les valeurs autorisées pour la taille de la clé sont `2048` , `3072` et `4096` . • Les périodes de validité sont de minimum 1 jour à maximum 36 500 jours. Même si une période de validité de 36 500 jours est autorisée, il est recommandé d'utiliser une période de validité ne dépassant pas 397 jours ou 13 mois. Car si vous sélectionnez une période de validité de plus de 397 jours et prévoyez d'exporter un CSR pour ce certificat et de le faire signer par une autorité de certification connue, la validité du certificat signé qui vous sera renvoyé par l'autorité de certification sera réduite à 397 jours. • Vous pouvez sélectionner la case à cocher « Exclure les informations d'identification locales (par exemple, localhost) » si vous souhaitez supprimer les informations d'identification locales du champ Noms alternatifs du certificat. Lorsque cette case à cocher est sélectionnée, seul ce que vous saisissez dans le champ est utilisé dans le champ Noms alternatifs. Si ce champ est laissé vide, le certificat résultant n'aura pas du tout de champ Noms alternatifs.

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

Redémarrer la machine virtuelle Unified Manager

Vous pouvez redémarrer la machine virtuelle à partir de la console de maintenance d'Unified Manager. Vous devez redémarrer après avoir généré un nouveau certificat de sécurité ou s'il y a un problème avec la machine virtuelle.

Avant de commencer

L'appareil virtuel est sous tension.

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

Vous pouvez également redémarrer la machine virtuelle à partir de vSphere en utilisant l'option **Redémarrer l'invité**. Consultez la documentation VMware pour plus d'informations.

Étapes

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

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

À un moment donné, vous souhaiterez peut-être modifier le nom d'hôte de la machine Red Hat Enterprise Linux sur laquelle vous avez installé Unified Manager. Par exemple, vous souhaiterez peut-être renommer l'hôte pour identifier plus facilement vos serveurs Unified Manager par type, groupe de travail ou groupe de cluster surveillé lorsque vous répertoriez 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 d'hôte (ou l'adresse IP de l'hôte) pour accéder à l'interface utilisateur Web d'Unified Manager. Si vous avez configuré une adresse IP statique pour votre réseau lors du déploiement, vous auriez alors désigné un nom pour l'hôte du réseau. Si vous avez configuré le réseau à l'aide de DHCP, le nom d'hôte doit être extrait du serveur DNS.

Quelle que soit la manière dont le nom d'hôte a été attribué, si vous modifiez le nom d'hôte et avez l'intention 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 en utilisant l'adresse IP du serveur au lieu du nom d'hôte, vous n'avez pas besoin de générer un nouveau certificat si vous modifiez le nom d'hôte. Cependant, il est recommandé de mettre à jour le certificat afin que le nom d'hôte dans le certificat corresponde au nom d'hôte réel. Le nouveau certificat ne prend effet qu'une fois la machine Linux 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. Arrêtez le logiciel Unified Manager et le logiciel MySQL associé en entrant la commande suivante :

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Changer le nom de l'hôte en utilisant 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 est capable de se pinger lui-même :

   ```
   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 le changement de nom d'hôte, redémarrez Unified Manager en entrant la commande suivante :

   ```
   systemctl start mysqld ocie ocieau
   ```

Informations sur le copyright

Copyright © 2025 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.