Description des fenêtres d'authentification et des boîtes de dialogue

OnCommand Unified Manager 9.5

NetApp
August 02, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/oncommand-unified-manager-95/online-help/reference-setup-authentication-page-um-7-3.html on August 02, 2024. Always check docs.netapp.com for the latest.

Sommaire

Description des fenêtres d’authentification et des boîtes de dialogue 1
Page Configuration/authentification 1
Page authentification à distance 1
Page authentification SAML 4

Description des fenêtres d’authentification et des boîtes de dialogue

Vous pouvez activer l’authentification LDAP à partir de la page Configuration/authentification.

Page Configuration/authentification

Vous pouvez utiliser la page installation/authentification pour configurer Unified Manager de manière à authentifier les utilisateurs distants qui tentent de se connecter à l’interface utilisateur Web d’Unified Manager.

La page authentification à distance vous permet de configurer Unified Manager pour qu’il communique avec votre serveur d’authentification afin d’authentifier les utilisateurs distants.

À l’aide de la page authentification SAML, vous pouvez configurer Unified Manager pour communiquer avec un fournisseur d’identité sécurisée (IDP) afin d’authentifier les utilisateurs distants.

Page authentification à distance

Vous pouvez utiliser la page authentification à distance pour configurer Unified Manager pour communiquer avec votre serveur d’authentification afin d’authentifier les utilisateurs distants qui tentent de se connecter à l’interface utilisateur Web Unified Manager.

Vous devez avoir le rôle d’administrateur OnCommand ou d’administrateur du stockage.

Après avoir sélectionné la case à cocher Activer l’authentification à distance, vous pouvez activer l’authentification à distance à l’aide d’un serveur d’authentification.

- **Service d’authentification**

  Vous permet de configurer le serveur de gestion pour authentifier les utilisateurs des fournisseurs de services d’annuaire, tels qu’Active Directory, OpenLDAP ou spécifier votre propre mécanisme d’authentification. Vous pouvez spécifier un service d’authentification uniquement si vous avez activé l’authentification à distance.

  - **Active Directory**
    - Nom de l’administrateur

      Indique le nom d’administrateur du serveur d’authentification.

    - Mot de passe

      Spécifie le mot de passe pour accéder au serveur d’authentification.

    - Nom unique de base

      Indique l’emplacement des utilisateurs distants dans le serveur d’authentification. Par exemple, si le nom de domaine du serveur d’authentification est ou@domain.com, le nom distinctif de base est `cn=ou,dc=domain,dc=com`.

- Désactiver la recherche de groupes imbriqués

  Indique s'il faut activer ou désactiver l'option de recherche de groupe imbriqué. Par défaut, cette option est désactivée. Si vous utilisez Active Directory, vous pouvez accélérer l'authentification en désactivant la prise en charge des groupes imbriqués.

- Utiliser connexion sécurisée

  Spécifie le service d'authentification utilisé pour communiquer avec les serveurs d'authentification.

- **OpenLDAP**
  - Lier le nom unique

    Spécifie le nom distinctif de liaison utilisé avec le nom distinctif de base pour trouver des utilisateurs distants dans le serveur d'authentification.

  - Lier le mot de passe

    Spécifie le mot de passe pour accéder au serveur d'authentification.

  - Nom unique de base

    Indique l'emplacement des utilisateurs distants dans le serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, le nom distinctif de base est `cn=ou,dc=domain,dc=com`.

  - Utiliser connexion sécurisée

    Indique que Secure LDAP est utilisé pour communiquer avec les serveurs d'authentification LDAPS.

- **Autres**
  - Lier le nom unique

    Spécifie le nom distinctif de liaison utilisé avec le nom distinctif de base pour trouver des utilisateurs distants dans le serveur d'authentification que vous avez configuré.

  - Lier le mot de passe

    Spécifie le mot de passe pour accéder au serveur d'authentification.

  - Nom unique de base

    Indique l'emplacement des utilisateurs distants dans le serveur d'authentification. Par exemple, si le nom de domaine du serveur d'authentification est ou@domain.com, le nom distinctif de base est `cn=ou,dc=domain,dc=com`.

  - Version du protocole

    Spécifie la version LDAP (Lightweight Directory Access Protocol) prise en charge par votre serveur d'authentification. Vous pouvez spécifier si la version du protocole doit être automatiquement détectée ou définir la version sur 2 ou 3.

  - Attribut de nom d'utilisateur

Spécifie le nom de l'attribut dans le serveur d'authentification qui contient les noms de connexion utilisateur à authentifier par le serveur de gestion.

- Attribut d'appartenance au groupe

  Spécifie une valeur qui attribue l'appartenance au groupe de serveurs de gestion aux utilisateurs distants en fonction d'un attribut et d'une valeur spécifiés dans le serveur d'authentification de l'utilisateur.

- UGID

  Si les utilisateurs distants sont inclus en tant que membres d'un objet groupeOfUniqueNames dans le serveur d'authentification, cette option vous permet d'affecter l'appartenance au groupe de serveurs de gestion aux utilisateurs distants en fonction d'un attribut spécifié dans cet objet groupeOfUniqueNames.

- Désactiver la recherche de groupes imbriqués

  Indique s'il faut activer ou désactiver l'option de recherche de groupe imbriqué. Par défaut, cette option est désactivée. Si vous utilisez Active Directory, vous pouvez accélérer l'authentification en désactivant la prise en charge des groupes imbriqués.

- Membre

  Indique le nom d'attribut utilisé par votre serveur d'authentification pour stocker des informations sur les membres individuels d'un groupe.

- Classe d'objets utilisateur

  Spécifie la classe d'objet d'un utilisateur dans le serveur d'authentification distant.

- Classe d'objet de groupe

  Spécifie la classe d'objet de tous les groupes du serveur d'authentification distant.

- Utiliser connexion sécurisée

  Spécifie le service d'authentification utilisé pour communiquer avec les serveurs d'authentification.

> Si vous souhaitez modifier le service d'authentification, assurez-vous de supprimer tout serveur d'authentification existant et d'ajouter de nouveaux serveurs d'authentification.

Zone serveurs d'authentification

La zone serveurs d'authentification affiche les serveurs d'authentification avec lesquels le serveur de gestion communique pour trouver et authentifier les utilisateurs distants. Les informations d'identification des utilisateurs ou groupes distants sont gérées par le serveur d'authentification.

- **Boutons de commande**

  Permet d'ajouter, de modifier ou de supprimer des serveurs d'authentification.

  - Autres

    Permet d'ajouter un serveur d'authentification.

Si le serveur d'authentification que vous ajoutez fait partie d'une paire haute disponibilité (à l'aide de la même base de données), vous pouvez également ajouter le serveur d'authentification partenaire. Cela permet au serveur de gestion de communiquer avec le partenaire lorsque l'un des serveurs d'authentification est inaccessible.

  - Modifier

    Permet de modifier les paramètres d'un serveur d'authentification sélectionné.

  - Supprimer

    Supprime les serveurs d'authentification sélectionnés.

- **Nom ou adresse IP**

  Affiche le nom d'hôte ou l'adresse IP du serveur d'authentification utilisé pour authentifier l'utilisateur sur le serveur de gestion.

- **Port**

  Affiche le numéro de port du serveur d'authentification.

- **Test d'authentification**

  Ce bouton valide la configuration de votre serveur d'authentification en authentifiant un utilisateur ou un groupe distant.

  Lors du test, si vous spécifiez uniquement le nom d'utilisateur, le serveur de gestion recherche l'utilisateur distant dans le serveur d'authentification, mais n'authentifie pas l'utilisateur. Si vous spécifiez à la fois le nom d'utilisateur et le mot de passe, le serveur de gestion recherche et authentifie l'utilisateur distant.

  Vous ne pouvez pas tester l'authentification si l'authentification à distance est désactivée.

Page authentification SAML

Vous pouvez utiliser la page SAML Authentication pour configurer Unified Manager afin d'authentifier les utilisateurs distants à l'aide de SAML via un fournisseur d'identités sécurisé avant de pouvoir vous connecter à l'interface utilisateur Web Unified Manager.

- Pour créer ou modifier la configuration SAML, vous devez avoir le rôle d'administrateur OnCommand.
- Vous devez avoir configuré l'authentification à distance.
- Vous devez avoir configuré au moins un utilisateur distant ou un groupe distant.

Une fois l'authentification à distance et les utilisateurs distants configurés, vous pouvez cocher la case Activer l'authentification SAML pour activer l'authentification à l'aide d'un fournisseur d'identité sécurisé.

- **URI IDP**

  URI permettant d'accéder au IDP à partir du serveur Unified Manager. Les exemples d'URI sont répertoriés ci-dessous.

  Exemple d'URI ADFS :

```
https://win2016-dc.ntap2016.local/federationmetadata/2007-
06/federationmetadata.xml
```

Exemple d'URI :

```
https://centos7.ntap2016.local/idp/shibboleth
```

- **Métadonnées IDP**

  Les métadonnées IDP au format XML.

  Si l'URL IDP est accessible à partir du serveur Unified Manager, vous pouvez cliquer sur le bouton **extraire les métadonnées IDP** pour remplir ce champ.

- **Système hôte (FQDN)**

  Le FQDN du système hôte Unified Manager tel que défini lors de l'installation. Vous pouvez modifier cette valeur si nécessaire.

- **URI hôte**

  URI permettant d'accéder au système hôte Unified Manager à partir du IDP.

- **Métadonnées hôte**

  Métadonnées du système hôte au format XML.

Informations sur le copyright

Copyright © 2024 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.