Gérer l'autorisation dynamique

ONTAP 9

NetApp
May 17, 2024

This PDF was generated from https://docs.netapp.com/fr-fr/ontap/authentication/dynamic-authorization-overview.html on May 17, 2024. Always check docs.netapp.com for the latest.

Sommaire

Gérer l’autorisation dynamique

Présentation de l’autorisation dynamique

À partir de ONTAP 9.15.1, les administrateurs peuvent configurer et activer l’autorisation dynamique afin d’accroître la sécurité de l’accès à distance à ONTAP, tout en limitant les dommages potentiels causés par un acteur malveillant. Avec ONTAP 9.15.1, l’autorisation dynamique fournit une structure initiale pour attribuer une note de sécurité aux utilisateurs et, si leur activité semble suspecte, les défier avec des vérifications d’autorisation supplémentaires ou refuser complètement une opération. Les administrateurs peuvent créer des règles, attribuer des scores de confiance et restreindre des commandes pour déterminer si certaines activités sont autorisées ou refusées pour un utilisateur. Les administrateurs peuvent activer l’autorisation dynamique à l’échelle du cluster ou pour des machines virtuelles de stockage individuelles.

Fonctionnement de l’autorisation dynamique

L’autorisation dynamique utilise un système de notation de confiance pour attribuer aux utilisateurs un niveau de confiance différent en fonction des stratégies d’autorisation. En fonction du niveau de confiance de l’utilisateur, une activité qu’il effectue peut être autorisée ou refusée, ou l’utilisateur peut être invité à demander une authentification supplémentaire.

Prenons l’exemple de trois utilisateurs différents qui tentent de supprimer un volume. Lorsqu’ils tentent d’effectuer l’opération, la cote de risque de chaque utilisateur est examinée :

- Le premier utilisateur se connecte à partir d’un appareil de confiance aux heures de bureau habituelles, ce qui rend son indice de risque faible ; l’opération est autorisée sans authentification supplémentaire.
- Le deuxième utilisateur se connecte à partir d’un appareil de confiance dans son domicile en dehors des heures de bureau, ce qui rend la note de risque modérée ; il est invité à demander une authentification supplémentaire avant que l’opération ne soit autorisée.
- Le troisième utilisateur se connecte à partir d’un appareil non approuvé dans un nouvel emplacement en dehors des heures de bureau, ce qui rend l’évaluation de risque élevée ; l’opération n’est pas autorisée.

Et la suite

- "Personnaliser l’autorisation dynamique"
- "Activer ou désactiver l’autorisation dynamique"

Activer ou désactiver l’autorisation dynamique

À partir de ONTAP 9.15.1, les administrateurs peuvent configurer et activer l’autorisation dynamique dans `visibility` pour tester la configuration, ou dans `enforced` Mode pour activer la configuration des utilisateurs de l’interface de ligne de commande qui se connectent via SSH. Si vous n’avez plus besoin d’une autorisation dynamique, vous pouvez la désactiver. Lorsque vous désactivez l’autorisation dynamique, les paramètres de configuration restent disponibles et vous pouvez les utiliser ultérieurement si vous décidez de la réactiver.

Pour plus d'informations sur les paramètres du `security dynamic-authorization modify` Reportez-vous aux pages de manuel ONTAP.

Activer l'autorisation dynamique pour les tests

Vous pouvez activer l'autorisation dynamique en mode visibilité, ce qui vous permet de tester la fonction et de vous assurer que les utilisateurs ne seront pas accidentellement verrouillés. Dans ce mode, le score de confiance est vérifié avec chaque activité restreinte, mais pas appliqué. Cependant, toute activité qui aurait été refusée ou qui aurait fait l'objet de défis d'authentification supplémentaires est consignée. Il est recommandé de tester les paramètres souhaités dans ce mode avant de les appliquer.

> Vous pouvez suivre cette étape pour activer l'autorisation dynamique pour la première fois, même si vous n'avez pas encore configuré d'autres paramètres d'autorisation dynamique. Reportez-vous à la section "Personnaliser l'autorisation dynamique" pour savoir comment configurer d'autres paramètres d'autorisation dynamique afin de les personnaliser en fonction de votre environnement.

Étapes

1. Activez l'autorisation dynamique en mode visibilité en configurant les paramètres globaux et en définissant l'état de la fonction sur `visibility`. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Vérifiez le résultat à l'aide de `show` commande pour afficher la configuration globale :

```
security dynamic-authorization show
```

Activer l'autorisation dynamique en mode imposé

Vous pouvez activer l'autorisation dynamique en mode imposé. En général, vous utilisez ce mode une fois les tests effectués en mode visibilité. Dans ce mode, le score de confiance est vérifié pour chaque activité restreinte et les restrictions d'activité sont appliquées si les conditions de restriction sont remplies. L'intervalle de suppression est également appliqué, ce qui évite des problèmes d'authentification supplémentaires dans l'intervalle spécifié.

> Cette étape suppose que vous avez précédemment configuré et activé l'autorisation dynamique dans `visibility` ce qui est fortement recommandé.

Étapes

1. Activer l'autorisation dynamique dans `enforced` en changeant son état à `enforced`. Si vous n'utilisez

pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization modify \
<strong>-state enforced</strong> \
-vserver <storage_VM_name>
```

2. Vérifiez le résultat à l'aide de `show` commande pour afficher la configuration globale :

```
security dynamic-authorization show
```

Désactiver l'autorisation dynamique

Vous pouvez désactiver l'autorisation dynamique si vous n'avez plus besoin de la sécurité d'authentification supplémentaire.

Étapes

1. Désactivez l'autorisation dynamique en changeant son état à `disabled`. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. Vérifiez le résultat à l'aide de `show` commande pour afficher la configuration globale :

```
security dynamic-authorization show
```

Et la suite

(Facultatif) en fonction de votre environnement, reportez-vous à la section "Personnaliser l'autorisation dynamique" pour configurer d'autres paramètres d'autorisation dynamique.

Personnaliser l'autorisation dynamique

En tant qu'administrateur, vous pouvez personnaliser différents aspects de votre configuration d'autorisation dynamique afin d'améliorer la sécurité des connexions SSH d'administrateur distant avec votre cluster ONTAP.

Vous pouvez personnaliser les paramètres d'autorisation dynamiques suivants en fonction de vos besoins en matière de sécurité :

- Configurer les paramètres globaux d'autorisation dynamique
- Configurer les composants de score de confiance d'autorisation dynamique
- Configurez un fournisseur de score de confiance personnalisé
- Configurer les commandes restreintes
- Configurer des groupes d'autorisation dynamiques

Configurer les paramètres globaux d'autorisation dynamique

Vous pouvez configurer des paramètres globaux pour l'autorisation dynamique, y compris la VM de stockage à sécuriser, l'intervalle de suppression pour les défis d'authentification et les paramètres de score de confiance.

Pour plus d'informations sur les paramètres et les valeurs par défaut du `security dynamic-authorization modify` Reportez-vous aux pages de manuel ONTAP.

Étapes

1. Configurer les paramètres globaux pour l'autorisation dynamique. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement :

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. Afficher la configuration résultante :

```
security dynamic-authorization show
```

Configurer les commandes restreintes

Lorsque vous activez l'autorisation dynamique, la fonction inclut un ensemble par défaut de commandes restreintes. Vous pouvez modifier cette liste en fonction de vos besoins. Reportez-vous à la "Documentation de vérification multiadministrateur" pour plus d'informations sur la liste par défaut des commandes restreintes.

Ajouter une commande restreinte

Vous pouvez ajouter une commande à la liste des commandes dont l'autorisation dynamique est limitée.

Pour plus d'informations sur les paramètres et les valeurs par défaut du `security dynamic-authorization rule create` Reportez-vous aux pages de manuel ONTAP.

Étapes

1. Ajoutez la commande. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization rule create \
-query <query> \
<strong>-operation <text></strong> \
-index <integer> \
-vserver <storage_VM_name>
```

2. Afficher la liste résultante des commandes restreintes :

```
security dynamic-authorization rule show
```

Supprime une commande restreinte

Vous pouvez supprimer une commande de la liste des commandes dont l'autorisation dynamique est limitée.

Pour plus d'informations sur les paramètres et les valeurs par défaut du `security dynamic-authorization rule delete` Reportez-vous aux pages de manuel ONTAP.

Étapes

1. Supprimez la commande. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization rule delete \
<strong>-operation <text></strong> \
-vserver <storage_VM_name>
```

2. Afficher la liste résultante des commandes restreintes :

```
security dynamic-authorization rule show
```

Configurer des groupes d'autorisation dynamiques

Par défaut, l'autorisation dynamique s'applique à tous les utilisateurs et groupes dès que vous l'activez. Toutefois, vous pouvez créer des groupes à l'aide de `security dynamic-authorization group create` de sorte que l'autorisation dynamique ne s'applique qu'à ces utilisateurs spécifiques.

Ajouter un groupe d'autorisation dynamique

Vous pouvez ajouter un groupe d'autorisation dynamique.

Pour plus d'informations sur les paramètres et les valeurs par défaut du `security dynamic-authorization group create` Reportez-vous aux pages de manuel ONTAP.

Étapes

1. Créez le groupe. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization group create \
<strong>-group-name <group-name></strong> \
-vserver <storage_VM_name> \
-exclude-users <user1,user2,user3...>
```

2. Afficher les groupes d'autorisation dynamiques résultants :

```
security dynamic-authorization group show
```

Supprimer un groupe d'autorisation dynamique

Vous pouvez supprimer un groupe d'autorisation dynamique.

Étapes

1. Supprimez le groupe. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization group delete \
<strong>-group-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. Afficher les groupes d'autorisation dynamiques résultants :

```
security dynamic-authorization group show
```

Configurer les composants de score de confiance d'autorisation dynamique

Vous pouvez configurer la pondération maximale du score pour modifier la priorité des critères de notation ou pour supprimer certains critères de l'évaluation du risque.

Dans le cadre de la meilleure pratique, vous devez laisser les valeurs de pondération par défaut en place et les ajuster uniquement si nécessaire.

Pour plus d'informations sur les paramètres et les valeurs par défaut du `security dynamic-authorization trust-score-component modify` Reportez-vous aux pages de manuel ONTAP.

Vous pouvez modifier les composants suivants, ainsi que leur score par défaut et leur pondération en pourcentage :

Critères	Nom du composant	Pondération de score brut par défaut	Poids en pourcentage par défaut
Périphérique de confiance	`trusted-device`	20	50
Historique d'authentification de connexion utilisateur	`authentication-history`	20	50

Étapes

1. Modifier les composants du score de confiance. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. Afficher les paramètres des composants du score de confiance obtenu :

```
security dynamic-authorization trust-score-component show
```

Réinitialiser le score de confiance d'un utilisateur

Si l'accès d'un utilisateur est refusé en raison de stratégies système et qu'il est capable de prouver son identité, l'administrateur peut réinitialiser le score de confiance de l'utilisateur.

Pour plus d'informations sur les paramètres et les valeurs par défaut du `security dynamic-authorization user-trust-score reset` Reportez-vous aux pages de manuel ONTAP.

Étapes

1. Ajoutez la commande. Reportez-vous à la section Configurer les composants de score de confiance d'autorisation dynamique pour obtenir une liste des composants de score de confiance que vous pouvez réinitialiser. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

Afficher votre score de confiance

Un utilisateur peut afficher son propre score de confiance pour une session de connexion.

Étapes

1. Afficher votre score de confiance :

```
security login whoami
```

Vous devez voir les résultats similaires à ce qui suit :

```
User: admin
Role: admin
Trust Score: 50
```

Configurez un fournisseur de score de confiance personnalisé

Si vous recevez déjà des méthodes de notation d'un fournisseur de score de confiance externe, vous pouvez ajouter le fournisseur personnalisé à la configuration d'autorisation dynamique.

Avant de commencer

- Le fournisseur de score de confiance personnalisé doit renvoyer une réponse JSON. Les conditions de syntaxe suivantes doivent être remplies :
  - Le champ qui renvoie le score de confiance doit être un champ scalaire et non un élément d'un tableau.
  - Le champ qui renvoie le score de confiance peut être un champ imbriqué, tel que `trust_score.value`.
  - Il doit y avoir un champ dans la réponse JSON qui renvoie un score de confiance numérique. Si ce n'est pas disponible en natif, vous pouvez écrire un script wrapper pour renvoyer cette valeur.
- La valeur fournie peut être un score de confiance ou un score de risque. La différence est que le score de confiance est dans l'ordre croissant avec un score plus élevé indiquant un niveau de confiance plus élevé, alors que le score de risque est dans l'ordre décroissant. Par exemple, un score de confiance de 90 pour une plage de scores de 0 à 100 indique que le score est très digne de confiance et qu'il est susceptible d'aboutir à un « Autoriser » sans défi supplémentaire, bien qu'un score de risque de 90 pour une plage de scores de 0 à 100 indique un risque élevé et risque de donner lieu à un « refus » sans défi supplémentaire.
- Le fournisseur de score de confiance personnalisé doit être accessible via l'API REST de ONTAP.
- Le fournisseur de score de confiance personnalisé doit être configurable à l'aide de l'un des paramètres pris en charge. Les fournisseurs de score de confiance personnalisés qui nécessitent une configuration ne figurant pas dans la liste des paramètres pris en charge ne sont pas pris en charge.

Pour plus d'informations sur les paramètres et les valeurs par défaut du `security dynamic-authorization trust-score-component create` Reportez-vous aux pages de manuel ONTAP.

Étapes

1. Ajoutez un fournisseur de score de confiance personnalisé. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. Afficher les paramètres du fournisseur de score de confiance :

```
security dynamic-authorization trust-score-component show
```

Configurer les balises de fournisseur de score de confiance personnalisé

Vous pouvez communiquer avec des fournisseurs externes de score de confiance à l'aide de balises. Cela vous permet d'envoyer des informations dans l'URL au fournisseur de score de confiance sans exposer d'informations sensibles.

Pour plus d'informations sur les paramètres et les valeurs par défaut du `security dynamic-authorization trust-score-component create` Reportez-vous aux pages de manuel ONTAP.

Étapes

1. Activer les balises de fournisseur de score de confiance. Mettez à jour les valeurs entre parenthèses <> pour les adapter à votre environnement. Si vous n'utilisez pas le `-vserver` paramètre, la commande est exécutée au niveau du cluster. Les paramètres en gras sont obligatoires :

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

Par exemple :

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

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.