Gestionar la autorización dinámica

ONTAP 9

NetApp
June 19, 2024

Tabla de contenidos

Gestionar la autorización dinámica 1
Descripción general de autorización dinámica 1
Activar o desactivar la autorización dinámica 1
Personalizar la autorización dinámica 3

Gestionar la autorización dinámica

Descripción general de autorización dinámica

A partir de ONTAP 9.15.1, los administradores pueden configurar y habilitar la autorización dinámica para aumentar la seguridad del acceso remoto a ONTAP al tiempo que se mitigan los daños potenciales que podría causar un agente malintencionado. Con ONTAP 9.15.1, la autorización dinámica proporciona un marco inicial para asignar una puntuación de seguridad a los usuarios y, si su actividad parece sospechosa, desafiarlos con comprobaciones de autorización adicionales o denegar una operación por completo. Los administradores pueden crear reglas, asignar puntuaciones de confianza y restringir comandos para determinar cuándo se permite o se deniega cierta actividad para un usuario. Los administradores pueden activar la autorización dinámica en todo el clúster o para máquinas virtuales de almacenamiento individuales.

Cómo funciona la autorización dinámica

La autorización dinámica utiliza un sistema de puntuación de confianza para asignar a los usuarios un nivel de confianza diferente en función de las políticas de autorización. Según el nivel de confianza del usuario, se puede permitir o denegar una actividad que realice, o se puede solicitar al usuario que realice una autenticación adicional.

Tome el ejemplo de tres usuarios diferentes que intentan eliminar un volumen. En el momento en que intentan realizar la operación, se examina la clasificación de riesgo para cada usuario:

- El primer usuario inicia sesión desde un dispositivo de confianza en horas normales de oficina, lo que hace que su calificación de riesgo sea baja; la operación se permite sin autenticación adicional.
- El segundo usuario inicia sesión desde un dispositivo de confianza en su casa fuera del horario de oficina, lo que hace que la calificación de riesgo sea moderada; se le solicita autenticación adicional antes de que se permita la operación.
- El tercer usuario inicia sesión desde un dispositivo que no es de confianza en una nueva ubicación fuera del horario de oficina, lo que hace que la clasificación de riesgo sea alta; la operación no está permitida.

El futuro

- "Personalizar la autorización dinámica"
- "Activar o desactivar la autorización dinámica"

Activar o desactivar la autorización dinámica

A partir de ONTAP 9.15.1, los administradores pueden configurar y activar la autorización dinámica en `visibility` modo para probar la configuración, o en `enforced` Modo para activar la configuración para usuarios de la CLI que se conectan a través de SSH. Si ya no necesita autorización dinámica, puede desactivarla. Cuando desactiva la autorización dinámica, los ajustes de configuración permanecen disponibles y puede utilizarlos más adelante si decide volver a habilitarla.

Para obtener más información acerca de los parámetros del `security dynamic-authorization modify`

Consulte las páginas del manual de ONTAP.

Active la autorización dinámica para realizar pruebas

Puede activar la autorización dinámica en el modo de visibilidad, lo que le permite probar la función y garantizar que los usuarios no se bloquearán accidentalmente. En este modo, la puntuación de confianza se comprueba con cada actividad restringida, pero no se aplica. Sin embargo, se registra cualquier actividad que hubiera sido denegada o sujeta a problemas de autenticación adicionales. Como práctica recomendada, debe probar la configuración deseada en este modo antes de aplicarla.

Puede seguir este paso para activar la autorización dinámica por primera vez, incluso si aún no ha configurado ninguna otra configuración de autorización dinámica. Consulte "Personalizar la autorización dinámica" para conocer los pasos necesarios para configurar otros valores de autorización dinámica para personalizarlos en su entorno.

Pasos

1. Active la autorización dinámica en el modo de visibilidad configurando los ajustes globales y cambiando el estado de la característica a. `visibility`. Si no utiliza el `-vserver` parámetro, el comando se ejecuta en el nivel del clúster. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Los parámetros en negrita son necesarios:

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

2. Compruebe el resultado mediante el `show` comando para mostrar la configuración global:

```
security dynamic-authorization show
```

Active la autorización dinámica en modo forzado

Puede activar la autorización dinámica en modo forzado. Normalmente, se utiliza este modo después de haber completado las pruebas con el modo de visibilidad. En este modo, la puntuación de confianza se comprueba con cada actividad restringida y las restricciones de actividad se aplican si se cumplen las condiciones de restricción. El intervalo de supresión también se aplica, lo que evita problemas de autenticación adicionales dentro del intervalo especificado.

Este paso supone que ha configurado y activado previamente la autorización dinámica en `visibility` modo, que se recomienda encarecidamente.

Pasos

1. Activar autorización dinámica en `enforced` el modo cambia su estado a. `enforced`. Si no utiliza el `-vserver` parámetro, el comando se ejecuta en el nivel del clúster. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Los parámetros en negrita son necesarios:

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

2. Compruebe el resultado mediante el `show` comando para mostrar la configuración global:

```
security dynamic-authorization show
```

Desactive la autorización dinámica

Puede desactivar la autorización dinámica si ya no necesita la seguridad de autenticación añadida.

Pasos

1. Desactive la autorización dinámica cambiando su estado a. `disabled`. Si no utiliza el `-vserver` parámetro, el comando se ejecuta en el nivel del clúster. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Los parámetros en negrita son necesarios:

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

2. Compruebe el resultado mediante el `show` comando para mostrar la configuración global:

```
security dynamic-authorization show
```

El futuro

(Opcional) Dependiendo del entorno, consulte "Personalizar la autorización dinámica" para configurar otros ajustes de autorización dinámica.

Personalizar la autorización dinámica

Como administrador, puede personalizar diferentes aspectos de su configuración de autorización dinámica para aumentar la seguridad de las conexiones SSH de administrador remoto al clúster de ONTAP.

Puede personalizar los siguientes ajustes de autorización dinámica en función de sus necesidades de seguridad:

- Configure los valores globales de autorización dinámica
- Configure los componentes de puntuación de confianza de autorización dinámica
- Configurar un proveedor de puntuación de confianza personalizado

- Configurar comandos restringidos
- Configurar grupos de autorización dinámicos

Configure los valores globales de autorización dinámica

Puede configurar valores globales para la autorización dinámica, incluida la máquina virtual de almacenamiento que se protegerá, el intervalo de supresión para los desafíos de autenticación y los ajustes de la puntuación de confianza.

Para obtener más información sobre los parámetros y los valores predeterminados de `security dynamic-authorization modify` Consulte las páginas del manual de ONTAP.

Pasos

1. Configure los valores globales para la autorización dinámica. Si no utiliza el `-vserver` parámetro, el comando se ejecuta en el nivel del clúster. Actualice los valores entre paréntesis <> para que coincidan con el entorno:

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

2. Vea la configuración resultante:

```
security dynamic-authorization show
```

Configurar comandos restringidos

Al activar la autorización dinámica, la función incluye un conjunto predeterminado de comandos restringidos. Puede modificar esta lista para adaptarla a sus necesidades. Consulte la "Documentación de verificación multi-admin (MAV)" para obtener información sobre la lista predeterminada de comandos restringidos.

Agregue un comando restringido

Puede agregar un comando a la lista de comandos restringidos con autorización dinámica.

Para obtener más información sobre los parámetros y los valores predeterminados de `security dynamic-authorization rule create` Consulte las páginas del manual de ONTAP.

Pasos

1. Agregue el comando. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no utiliza el `-vserver` parámetro, el comando se ejecuta en el nivel del clúster. Los parámetros en negrita son necesarios:

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

2. Vea la lista resultante de comandos restringidos:

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

Eliminar un comando restringido

Puede eliminar un comando de la lista de comandos restringidos con autorización dinámica.

Para obtener más información sobre los parámetros y los valores predeterminados de `security dynamic-authorization rule delete` Consulte las páginas del manual de ONTAP.

Pasos

1. Quite el comando. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no utiliza el `-vserver` parámetro, el comando se ejecuta en el nivel del clúster. Los parámetros en negrita son necesarios:

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

2. Vea la lista resultante de comandos restringidos:

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

Configurar grupos de autorización dinámicos

De forma predeterminada, la autorización dinámica se aplica a todos los usuarios y grupos tan pronto como la habilite. Sin embargo, puede crear grupos con `security dynamic-authorization group create` de modo que la autorización dinámica solo se aplica a esos usuarios específicos.

Agregue un grupo de autorización dinámica

Puede agregar un grupo de autorización dinámica.

Para obtener más información sobre los parámetros y los valores predeterminados de `security dynamic-authorization group create` Consulte las páginas del manual de ONTAP.

Pasos

1. Cree el grupo. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no utiliza el `-vserver` parámetro, el comando se ejecuta en el nivel del clúster. Los parámetros en negrita son necesarios:

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

2. Vea los grupos de autorización dinámica resultantes:

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

Eliminar un grupo de autorización dinámica

Puede eliminar un grupo de autorización dinámica.

Pasos

1. Elimine el grupo. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no utiliza el `-vserver` parámetro, el comando se ejecuta en el nivel del clúster. Los parámetros en negrita son necesarios:

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

2. Vea los grupos de autorización dinámica resultantes:

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

Configure los componentes de puntuación de confianza de autorización dinámica

Puede configurar el peso máximo de puntuación para cambiar la prioridad de los criterios de puntuación o para eliminar determinados criterios de la puntuación de riesgo.

Como práctica recomendada, debe dejar los valores predeterminados de ponderación de puntuación en su lugar y ajustarlos solo si es necesario.

Para obtener más información sobre los parámetros y los valores predeterminados de `security dynamic-authorization trust-score-component modify` Consulte las páginas del manual de ONTAP.

Los siguientes son los componentes que puede modificar, junto con su puntuación predeterminada y sus ponderaciones porcentuales:

Criterios	Nombre del componente	Peso bruto por defecto de la puntuación	Peso porcentual predeterminado
Dispositivo de confianza	`trusted-device`	20	50
Historial de autenticación de inicio de sesión de usuario	`authentication-history`	20	50

Pasos

1. Modificar componentes de puntuación de confianza. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no utiliza el `-vserver` parámetro, el comando se ejecuta en el nivel del clúster. Los parámetros en negrita son necesarios:

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

2. Vea la configuración del componente de puntuación de confianza resultante:

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

Restablezca la puntuación de confianza de un usuario

Si se deniega el acceso a un usuario debido a políticas del sistema y es capaz de probar su identidad, el administrador puede restablecer la puntuación de confianza del usuario.

Para obtener más información sobre los parámetros y los valores predeterminados de `security dynamic-authorization user-trust-score reset` Consulte las páginas del manual de ONTAP.

Pasos

1. Agregue el comando. Consulte Configure los componentes de puntuación de confianza de autorización dinámica para obtener una lista de componentes de puntuación de confianza que puede restablecer. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no utiliza el `-vserver` parámetro, el comando se ejecuta en el nivel del clúster. Los parámetros en negrita son necesarios:

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

Muestra tu puntuación de confianza

Un usuario puede mostrar su propia puntuación de confianza para una sesión de conexión.

Pasos

1. Mostrar su puntuación de confianza:

```
security login whoami
```

Debería ver una salida similar a la siguiente:

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

Configurar un proveedor de puntuación de confianza personalizado

Si ya recibe métodos de puntuación de un proveedor de puntuación de confianza externo, puede agregar el proveedor personalizado a la configuración de autorización dinámica.

Antes de empezar

- El proveedor de puntuación de confianza personalizado debe devolver una respuesta JSON. Deben cumplirse los siguientes requisitos de sintaxis:
  - El campo que devuelve la puntuación de confianza debe ser un campo escalar y no un elemento de una matriz.
  - El campo que devuelve la puntuación de confianza puede ser un campo anidado, como `trust_score.value`.
  - Debe haber un campo dentro de la respuesta JSON que devuelva una puntuación de confianza numérica. Si esto no está disponible de forma nativa, puede escribir un script de contenedor para devolver este valor.
- El valor proporcionado puede ser una puntuación de confianza o una puntuación de riesgo. La diferencia es que la puntuación de confianza está en orden ascendente con una puntuación más alta que indica un nivel de confianza más alto, mientras que la puntuación de riesgo está en orden descendente. Por ejemplo, una puntuación de confianza de 90 para un rango de puntuación de 0 a 100 indica que la puntuación es muy confiable y probable que resulte en un “permiso” sin desafío adicional, mientras que una puntuación de riesgo de 90 para un rango de puntuación de 0 a 100 indica un alto riesgo y es probable que resulte en una “denegación” sin un desafío adicional.
- Se debe poder acceder al proveedor de puntuación de confianza personalizado a través de la API DE REST DE ONTAP.
- El proveedor de puntuación de confianza personalizada debe configurarse mediante uno de los parámetros admitidos. No se admiten los proveedores de puntuación de confianza personalizados que requieren una configuración que no esté en la lista de parámetros soportados.

Para obtener más información sobre los parámetros y los valores predeterminados de `security dynamic-authorization trust-score-component create` Consulte las páginas del manual de ONTAP.

Pasos

1. Agregar un proveedor de puntuación de confianza personalizado. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no utiliza el `-vserver` parámetro, el comando se ejecuta en el nivel del clúster. Los parámetros en negrita son necesarios:

```
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. Vea la configuración del proveedor de puntuación de confianza resultante:

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

Configurar etiquetas personalizadas de proveedor de puntuación de confianza

Puede comunicarse con proveedores de puntuación de confianza externos mediante etiquetas. Esto le permite enviar información en la URL al proveedor de puntuación de confianza sin exponer información confidencial.

Para obtener más información sobre los parámetros y los valores predeterminados de `security dynamic-authorization trust-score-component create` Consulte las páginas del manual de ONTAP.

Pasos

1. Activar etiquetas de proveedor de puntuación de confianza. Actualice los valores entre paréntesis <> para que coincidan con el entorno. Si no utiliza el `-vserver` parámetro, el comando se ejecuta en el nivel del clúster. Los parámetros en negrita son necesarios:

```
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>
```

Por ejemplo:

```
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"
```

Información de copyright

Información de la marca comercial