Dynamische Autorisierung verwalten

ONTAP 9

NetApp
June 19, 2024

Inhalt

Dynamische Autorisierung verwalten

Dynamische Autorisierung – Übersicht

Ab ONTAP 9.15.1 können Administratoren dynamische Autorisierungen konfigurieren und aktivieren, um die Sicherheit des Remote-Zugriffs auf ONTAP zu erhöhen und gleichzeitig potenzielle Schäden zu minimieren, die durch einen böswilligen Akteur verursacht werden können. Mit ONTAP 9.15.1 bietet die dynamische Autorisierung einen ersten Rahmen für die Zuweisung einer Sicherheitsbewertung für Benutzer. Wenn ihre Aktivität verdächtig aussieht, werden sie durch zusätzliche Berechtigungsprüfungen oder die völlige Ablehnung eines Vorgangs in Frage gestellt. Administratoren können Regeln erstellen, Vertrauenswerte zuweisen und Befehle einschränken, um zu bestimmen, wann bestimmte Aktivitäten für einen Benutzer zugelassen oder verweigert werden. Administratoren können Cluster-weit oder für einzelne Storage VMs eine dynamische Autorisierung aktivieren.

Wie die dynamische Autorisierung funktioniert

Die dynamische Autorisierung verwendet ein System zur Vertrauensbewertung, um Benutzern je nach den Autorisierungsrichtlinien eine andere Vertrauensebene zuzuweisen. Je nach Vertrauensstufe des Benutzers kann eine Aktivität, die er durchführt, zugelassen oder verweigert werden, oder der Benutzer kann zur weiteren Authentifizierung aufgefordert werden.

Nehmen wir das Beispiel von drei verschiedenen Benutzern, die versuchen, ein Volume zu löschen. Bei dem Versuch, den Vorgang durchzuführen, wird die Risikoeinstufung für jeden Benutzer untersucht:

- Der erste Benutzer meldet sich von einem vertrauenswürdigen Gerät zu normalen Geschäftszeiten an, wodurch seine Risikoeinstufung gering wird. Der Vorgang ist ohne zusätzliche Authentifizierung zulässig.
- Der zweite Benutzer meldet sich außerhalb der Bürozeiten von einem vertrauenswürdigen Gerät in seinem Haus an, was die Risikoeinstufung moderat macht. Er wird aufgefordert, eine zusätzliche Authentifizierung durchzuführen, bevor der Vorgang zugelassen wird.
- Der dritte Benutzer meldet sich von einem nicht vertrauenswürdigen Gerät außerhalb der Bürozeiten an einem neuen Standort an, wodurch die Risikoeinstufung hoch ist. Der Vorgang ist nicht zulässig.

Wie es weiter geht

- "Dynamische Autorisierung anpassen"
- "Aktivieren oder Deaktivieren der dynamischen Autorisierung"

Aktivieren oder Deaktivieren der dynamischen Autorisierung

Ab ONTAP 9.15.1 können Administratoren die dynamische Autorisierung in konfigurieren und aktivieren `visibility` Modus zum Testen der Konfiguration oder in `enforced` Modus zum Aktivieren der Konfiguration für CLI-Benutzer, die sich über SSH verbinden. Wenn Sie keine dynamische Autorisierung mehr benötigen, können Sie diese deaktivieren. Wenn Sie die dynamische Autorisierung deaktivieren, bleiben die

Konfigurationseinstellungen verfügbar, und Sie können sie später verwenden, wenn Sie sie erneut aktivieren möchten.

Weitere Informationen zu den Parametern für das `security dynamic-authorization modify` Finden Sie weitere Informationen in den ONTAP-Handbuchseiten.

Dynamische Autorisierung für Tests aktivieren

Sie können die dynamische Autorisierung im Sichtbarkeitsmodus aktivieren, sodass Sie die Funktion testen und sicherstellen können, dass Benutzer nicht versehentlich gesperrt werden. In diesem Modus wird die Vertrauensbewertung mit jeder eingeschränkten Aktivität überprüft, jedoch nicht erzwungen. Jede Aktivität, die abgelehnt worden wäre oder zusätzlichen Authentifizierungsherausforderungen unterliegen würde, wird jedoch protokolliert. Als Best Practice sollten Sie die beabsichtigten Einstellungen in diesem Modus testen, bevor Sie sie durchsetzen.

> Sie können diesen Schritt ausführen, um die dynamische Autorisierung zum ersten Mal zu aktivieren, auch wenn Sie noch keine anderen dynamischen Autorisierungseinstellungen konfiguriert haben. Siehe "Dynamische Autorisierung anpassen" Hier finden Sie Schritte zum Konfigurieren anderer dynamischer Autorisierungseinstellungen, um sie an Ihre Umgebung anzupassen.

Schritte

1. Aktivieren Sie die dynamische Autorisierung im Sichtbarkeitsmodus, indem Sie globale Einstellungen konfigurieren und den Funktionsstatus in ändern `visibility`. Wenn Sie den nicht verwenden `-vserver` Parameter, der Befehl wird auf Cluster-Ebene ausgeführt. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Fett formatierte Parameter sind erforderlich:

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

2. Überprüfen Sie das Ergebnis mithilfe der `show` Befehl zum Anzeigen der globalen Konfiguration:

```
security dynamic-authorization show
```

Dynamische Autorisierung im erzwungenen Modus aktivieren

Sie können die dynamische Autorisierung im erzwungenen Modus aktivieren. In der Regel verwenden Sie diesen Modus, nachdem Sie die Tests im Sichtmodus abgeschlossen haben. In diesem Modus wird die Vertrauensbewertung mit jeder eingeschränkten Aktivität überprüft, und Aktivitätsbeschränkungen werden erzwungen, wenn die Bedingungen für Einschränkungen erfüllt sind. Das Unterdrückungsintervall wird ebenfalls erzwungen, wodurch zusätzliche Authentifizierungsherausforderungen innerhalb des angegebenen Intervalls verhindert werden.

Bei diesem Schritt wird davon ausgegangen, dass Sie die dynamische Autorisierung in zuvor konfiguriert und aktiviert haben `visibility` Modus, der dringend empfohlen wird.

Schritte

1. Dynamische Autorisierung in aktivieren `enforced` Modus, indem ihr Status in geändert wird `enforced`. Wenn Sie den nicht verwenden `-vserver` Parameter, der Befehl wird auf Cluster-Ebene ausgeführt. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Fett formatierte Parameter sind erforderlich:

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

2. Überprüfen Sie das Ergebnis mithilfe der `show` Befehl zum Anzeigen der globalen Konfiguration:

```
security dynamic-authorization show
```

Dynamische Autorisierung deaktivieren

Sie können die dynamische Autorisierung deaktivieren, wenn Sie die zusätzliche Authentifizierungssicherheit nicht mehr benötigen.

Schritte

1. Deaktivieren Sie die dynamische Autorisierung, indem Sie den Status in ändern `disabled`. Wenn Sie den nicht verwenden `-vserver` Parameter, der Befehl wird auf Cluster-Ebene ausgeführt. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Fett formatierte Parameter sind erforderlich:

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

2. Überprüfen Sie das Ergebnis mithilfe der `show` Befehl zum Anzeigen der globalen Konfiguration:

```
security dynamic-authorization show
```

Wie es weiter geht

(Optional) je nach Umgebung finden Sie unter "Dynamische Autorisierung anpassen" Um andere dynamische Autorisierungseinstellungen zu konfigurieren.

Dynamische Autorisierung anpassen

Als Administrator können Sie verschiedene Aspekte Ihrer dynamischen Autorisierungskonfiguration anpassen, um die Sicherheit von SSH-Verbindungen des Remote-Administrators zu Ihrem ONTAP-Cluster zu erhöhen.

Sie können die folgenden dynamischen Autorisierungseinstellungen je nach Ihren Sicherheitsanforderungen anpassen:

- Konfigurieren Sie die globalen Einstellungen für die dynamische Autorisierung
- Konfigurieren Sie die Komponenten für die dynamische Autorisierung der Vertrauensbewertung
- Konfigurieren Sie einen benutzerdefinierten Anbieter für Vertrauensbewertung
- Eingeschränkte Befehle konfigurieren
- Konfigurieren Sie dynamische Autorisierungsgruppen

Konfigurieren Sie die globalen Einstellungen für die dynamische Autorisierung

Sie können globale Einstellungen für die dynamische Autorisierung konfigurieren, einschließlich der zu sicheren Speicher-VM, des Unterdrückungsintervalls für Authentifizierungsherausforderungen und der Einstellungen für die Vertrauensbewertung.

Weitere Informationen zu den Parametern und Standardwerten für das `security dynamic-authorization modify` Finden Sie weitere Informationen in den ONTAP-Handbuchseiten.

Schritte

1. Konfigurieren Sie globale Einstellungen für dynamische Autorisierung. Wenn Sie den nicht verwenden `-vserver` Parameter, der Befehl wird auf Cluster-Ebene ausgeführt. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen:

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

2. Die resultierende Konfiguration anzeigen:

```
security dynamic-authorization show
```

Eingeschränkte Befehle konfigurieren

Wenn Sie die dynamische Autorisierung aktivieren, enthält die Funktion einen Standardsatz von eingeschränkten Befehlen. Sie können diese Liste an Ihre Bedürfnisse anpassen. Siehe "Multi-Admin Verification (MAV)-Dokumentation" Für Informationen zur Standardliste der eingeschränkten Befehle.

Fügen Sie einen eingeschränkten Befehl hinzu

Sie können der Liste der Befehle, die durch dynamische Autorisierung eingeschränkt sind, einen Befehl hinzufügen.

Weitere Informationen zu den Parametern und Standardwerten für das `security dynamic-authorization rule create` Finden Sie weitere Informationen in den ONTAP-Handbuchseiten.

Schritte

1. Fügen Sie den Befehl hinzu. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den nicht verwenden `-vserver` Parameter, der Befehl wird auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

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

2. Zeigt die resultierende Liste der eingeschränkten Befehle an:

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

Entfernen Sie einen eingeschränkten Befehl

Sie können einen Befehl aus der Liste der Befehle entfernen, die mit dynamischer Autorisierung eingeschränkt sind.

Weitere Informationen zu den Parametern und Standardwerten für das `security dynamic-authorization rule delete` Finden Sie weitere Informationen in den ONTAP-Handbuchseiten.

Schritte

1. Entfernen Sie den Befehl. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den nicht verwenden `-vserver` Parameter, der Befehl wird auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

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

2. Zeigt die resultierende Liste der eingeschränkten Befehle an:

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

Konfigurieren Sie dynamische Autorisierungsgruppen

Standardmäßig gilt die dynamische Autorisierung für alle Benutzer und Gruppen, sobald Sie sie aktivieren. Sie können jedoch Gruppen mit dem erstellen `security dynamic-authorization group create` So dass die dynamische Autorisierung nur für bestimmte Benutzer gilt.

Fügen Sie eine dynamische Autorisierungsgruppe hinzu

Sie können eine dynamische Autorisierungsgruppe hinzufügen.

Weitere Informationen zu den Parametern und Standardwerten für das `security dynamic-authorization group create` Finden Sie weitere Informationen in den ONTAP-Handbuchseiten.

Schritte

1. Erstellen Sie die Gruppe. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den nicht verwenden `-vserver` Parameter, der Befehl wird auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

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

2. Anzeigen der resultierenden dynamischen Autorisierungsgruppen:

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

Entfernen einer dynamischen Berechtigungsgruppe

Sie können eine dynamische Autorisierungsgruppe entfernen.

Schritte

1. Löschen Sie die Gruppe. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den nicht verwenden `-vserver` Parameter, der Befehl wird auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

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

2. Anzeigen der resultierenden dynamischen Autorisierungsgruppen:

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

Konfigurieren Sie die Komponenten für die dynamische Autorisierung der Vertrauensbewertung

Sie können die maximale Gewichtung der Bewertung konfigurieren, um die Priorität der Bewertungskriterien zu ändern oder bestimmte Kriterien aus der Risikobewertung zu entfernen.

> Als Best Practice sollten Sie die Standardwerte für die Gewichtung der Punktzahl beibehalten und nur bei Bedarf anpassen.

Weitere Informationen zu den Parametern und Standardwerten für das `security dynamic-authorization trust-score-component modify` Finden Sie weitere Informationen in den ONTAP-Handbuchseiten.

Im Folgenden finden Sie die Komponenten, die Sie zusammen mit der Standardbewertung und den Prozentgewichtungen ändern können:

Kriterien	Komponentenname	Standardgewicht für Rohwert	Standardgewichtung in Prozent
Vertrauenswürdiges Gerät	`trusted-device`	20	50
Authentifizierungsverlauf der Benutzeranmeldung	`authentication-history`	20	50

Schritte

1. Komponenten der Vertrauensbewertung ändern. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den nicht verwenden `-vserver` Parameter, der Befehl wird auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

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

2. Anzeigen der resultierenden Komponenteneinstellungen für die Vertrauensbewertung:

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

Setzt die Vertrauensbewertung für einen Benutzer zurück

Wenn einem Benutzer aufgrund von Systemrichtlinien der Zugriff verweigert wird und seine Identität nachgewiesen werden kann, kann der Administrator die Vertrauensbewertung des Benutzers zurücksetzen.

Weitere Informationen zu den Parametern und Standardwerten für das `security dynamic-authorization user-trust-score reset` Finden Sie weitere Informationen in den ONTAP-Handbuchseiten.

Schritte

1. Fügen Sie den Befehl hinzu. Siehe Konfigurieren Sie die Komponenten für die dynamische Autorisierung

der Vertrauensbewertung Für eine Liste der Komponenten der Vertrauensbewertung, die Sie zurücksetzen können. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den nicht verwenden `-vserver` Parameter, der Befehl wird auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

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

Zeigen Sie Ihre Vertrauensbewertung an

Ein Benutzer kann seine eigene Vertrauensbewertung für eine Anmeldesitzung anzeigen.

Schritte

1. Ihr Vertrauenswert anzeigen:

```
security login whoami
```

Sie sollten eine Ausgabe wie die folgende sehen:

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

Konfigurieren Sie einen benutzerdefinierten Anbieter für Vertrauensbewertung

Wenn Sie bereits Bewertungsmethoden von einem externen Anbieter für Vertrauensbewertungen erhalten, können Sie den benutzerdefinierten Anbieter der dynamischen Autorisierungskonfiguration hinzufügen.

Bevor Sie beginnen

- Der benutzerdefinierte Anbieter für Vertrauensbewertung muss eine JSON-Antwort zurückgeben. Folgende Syntaxanforderungen müssen erfüllt sein:
  - Das Feld, das die Vertrauensstellung zurückgibt, muss ein skalares Feld sein und kein Element eines Arrays.
  - Das Feld, das die Vertrauensbewertung zurückgibt, kann ein verschachteltes Feld sein, z. B. `trust_score.value`.
  - In der JSON-Antwort muss ein Feld vorhanden sein, das eine numerische Vertrauensbewertung zurückgibt. Wenn dies nicht nativ verfügbar ist, können Sie ein Wrapper-Skript schreiben, um diesen Wert zurückzugeben.
- Der angegebene Wert kann entweder eine Vertrauensbewertung oder eine Risikobewertung sein. Der Unterschied besteht darin, dass die Vertrauensbewertung in aufsteigender Reihenfolge erfolgt, wobei eine höhere Bewertung ein höheres Vertrauensniveau bedeutet, während die Risikobewertung in absteigender Reihenfolge erfolgt. Ein Vertrauenswert von 90 für einen Score-Bereich von 0 bis 100 zeigt beispielsweise an, dass die Bewertung sehr vertrauenswürdig ist und wahrscheinlich zu einem „Zulassen“ ohne

zusätzliche Herausforderung führt. während ein Risiko-Score von 90 für einen Score-Bereich von 0 bis 100 auf ein hohes Risiko hinweist und wahrscheinlich zu einem „Deny“ ohne zusätzliche Herausforderung führt.

- Auf den benutzerdefinierten Anbieter für die Vertrauensbewertung muss über die ONTAP-REST-API zugegriffen werden können.
- Der benutzerdefinierte Anbieter für die Vertrauensbewertung muss mit einem der unterstützten Parameter konfiguriert werden. Benutzerdefinierte Anbieter von Vertrauensbewertungen, die eine Konfiguration erfordern, die nicht in der unterstützten Parameterliste enthalten ist, werden nicht unterstützt.

Weitere Informationen zu den Parametern und Standardwerten für das `security dynamic-authorization trust-score-component create` Finden Sie weitere Informationen in den ONTAP-Handbuchseiten.

Schritte

1. Fügen Sie einen benutzerdefinierten Anbieter für Vertrauensbewertung hinzu. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den nicht verwenden `-vserver` Parameter, der Befehl wird auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

```
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. Die resultierenden Einstellungen für den Anbieter der Vertrauensbewertung anzeigen:

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

Konfigurieren Sie benutzerdefinierte Provider-Tags für die Vertrauensbewertung

Sie können mit externen Anbietern von Vertrauensbewertungen über Tags kommunizieren. Auf diese Weise können Sie Informationen in der URL an den Anbieter der Vertrauensstellung senden, ohne vertrauliche Informationen preiszugeben.

Weitere Informationen zu den Parametern und Standardwerten für das `security dynamic-authorization trust-score-component create` Finden Sie weitere Informationen in den ONTAP-Handbuchseiten.

Schritte

1. Aktivieren Sie die Tags für Anbieter von Vertrauensbewertung. Aktualisieren Sie die Werte in Klammern <>, um sie an Ihre Umgebung anzupassen. Wenn Sie den nicht verwenden `-vserver` Parameter, der Befehl wird auf Cluster-Ebene ausgeführt. Fett formatierte Parameter sind erforderlich:

```
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>
```

Beispiel:

```
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"
```