管理动态授权
ONTAP 9

NetApp
June 19, 2024

目录

管理动态授权

动态授权概述

从ONTAP 9.151开始、管理员可以配置和启用动态授权、以提高远程访问ONTAP的安全性、同时缓解恶意攻击者可能造成的潜在损害。在ONTAP 9.151中、动态授权提供了一个初始框架、用于为用户分配安全得分、如果用户的活动看起来可疑、则通过额外的授权检查向用户提出质疑或完全拒绝操作。管理员可以创建规则、分配信任得分和限制命令、以确定何时允许或拒绝用户执行某些活动。管理员可以在集群范围内启用动态授权、也可以为各个Storage VM启用动态授权。

动态授权的工作原理

动态授权使用信任评分系统根据授权策略为用户分配不同的信任级别。根据用户的信任级别、可以允许或拒绝他们执行的活动、也可以提示用户进行进一步的身份验证。

以三个不同用户尝试删除卷为例。在尝试执行操作时、会检查每个用户的风险等级：

- 第一个用户在正常工作时间从可信设备登录、这使她的风险等级较低；无需额外身份验证即可操作。
- 第二位用户在办公时间之外从家中的可信设备登录、这使风险评级为中等；在允许执行此操作之前、系统会提示她进行额外的身份验证。
- 第三个用户在非工作时间从不可信的设备登录到新位置、这会使风险等级较高；不允许执行此操作。

下一步行动

- "自定义动态授权"
- "启用或禁用动态授权"

启用或禁用动态授权

从ONTAP 9.15.1开始、管理员可以在中配置和启用动态授权 `visibility` 用于测试配置的模式、或在中 `enforced` 用于为通过SSH连接的CLI用户激活配置的模式。如果您不再需要动态授权、可以将其禁用。禁用动态授权后、配置设置仍可用、如果您决定重新启用、可以稍后使用这些设置。

有关参数的详细信息、请参见 `security dynamic-authorization modify` 命令、请参阅ONTAP手册页。

为测试启用动态授权

您可以在可见性模式下启用动态授权、以便测试此功能并确保用户不会意外锁定。在此模式下、系统会对每个受限活动检查信任得分、但不会强制执行此得分。但是、系统会记录任何可能会被拒绝或面临其他身份验证挑战的活动。作为最佳实践、您应在此模式下测试所需设置、然后再强制实施。

> 即使尚未配置任何其他动态授权设置、也可以按照此步骤首次启用动态授权。请参见 "自定义动态授权" 了解配置其他动态授权设置以根据您的环境对其进行自定义的步骤。

步骤

1. 通过配置全局设置并将功能状态更改为、在可见性模式下启用动态授权 `visibility`。如果不使用 `-vserver` 参数、则命令将在集群级别运行。更新括号<>中的值以匹配您的环境。参数必须以粗体显示：

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

2. 使用检查结果 `show` 命令以显示全局配置：

```
security dynamic-authorization show
```

在强制模式下启用动态授权

您可以在强制模式下启用动态授权。通常、在使用可见性模式完成测试后、您会使用此模式。在此模式下、系统会对每个受限活动检查信任得分、如果满足限制条件、则会强制实施活动限制。此外、还会强制实施禁止间隔、以防止在指定间隔内出现其他身份验证问题。

此步骤假定您之前已在中配置并启用动态授权 `visibility` 模式、强烈建议使用此模式。

步骤

1. 在中启用动态授权 `enforced` 模式、方法是将其状态更改为 `enforced`。如果不使用 `-vserver` 参数、则命令将在集群级别运行。更新括号<>中的值以匹配您的环境。参数必须以粗体显示：

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

2. 使用检查结果 `show` 命令以显示全局配置：

```
security dynamic-authorization show
```

禁用动态授权

如果您不再需要添加的身份验证安全性、则可以禁用动态授权。

步骤

1. 通过将动态授权的状态更改为来禁用它 `disabled`。如果不使用 `-vserver` 参数、则命令将在集群级别运

行。更新括号<>中的值以匹配您的环境。参数必须以粗体显示：

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

2. 使用检查结果 `show` 命令以显示全局配置：

```
security dynamic-authorization show
```

下一步行动

(可选)根据您的环境、请参见 "自定义动态授权" 配置其他动态授权设置。

自定义动态授权

作为管理员、您可以自定义动态授权配置的不同方面、以提高远程管理员与ONTAP集群的SSH连接的安全性。

您可以根据安全需求自定义以下动态授权设置：

- [配置动态授权全局设置]
- [配置动态授权信任得分组件]
- [配置自定义信任得分提供程序]
- [配置受限命令]
- [配置动态授权组]

配置动态授权全局设置

您可以配置动态授权的全局设置、包括要保护的Storage VM、身份验证挑战的禁止间隔以及信任得分设置。

有关的参数和默认值的详细信息 `security dynamic-authorization modify` 命令、请参阅ONTAP手册页。

步骤

1. 配置动态授权的全局设置。如果不使用 `-vserver` 参数、则命令将在集群级别运行。更新括号<>中的值以符合您的环境：

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

2. 查看生成的配置：

```
security dynamic-authorization show
```

配置受限命令

启用动态授权后、此功能将包括一组默认的受限命令。您可以根据需要修改此列表。请参见 "多管理员验证(MAV)文档" 有关默认受限命令列表的信息。

添加受限命令

您可以将命令添加到受动态授权限制的命令列表中。

有关的参数和默认值的详细信息 `security dynamic-authorization rule create` 命令、请参阅ONTAP手册页。

步骤

1. 添加命令。更新括号<>中的值以匹配您的环境。如果不使用 `-vserver` 参数、则命令将在集群级别运行。参数必须以粗体显示：

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

2. 查看生成的受限命令列表：

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

删除受限命令

您可以从受动态授权限制的命令列表中删除命令。

有关的参数和默认值的详细信息 `security dynamic-authorization rule delete` 命令、请参阅ONTAP手册页。

步骤

1. 删除命令。更新括号<>中的值以匹配您的环境。如果不使用 `-vserver` 参数、则命令将在集群级别运行。参数必须以粗体显示：

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

2. 查看生成的受限命令列表：

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

配置动态授权组

默认情况下、动态授权会在启用后立即适用场景所有用户和组。但是、您可以使用创建组 `security dynamic-authorization group create` 命令、以便动态授权仅适用场景这些特定用户。

添加动态授权组

您可以添加动态授权组。

有关的参数和默认值的详细信息 `security dynamic-authorization group create` 命令、请参阅ONTAP手册页。

步骤

1. 创建组。更新括号<>中的值以匹配您的环境。如果不使用 `-vserver` 参数、则命令将在集群级别运行。参数必须以粗体显示：

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

2. 查看生成的动态授权组：

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

删除动态授权组

您可以删除动态授权组。

步骤

1. 删除组。更新括号<>中的值以匹配您的环境。如果不使用 `-vserver` 参数、则命令将在集群级别运行。参

数必须以粗体显示：

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

2. 查看生成的动态授权组：

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

配置动态授权信任得分组件

您可以配置最大分数权重、以更改评分标准的优先级或从风险评分中删除某些标准。

作为最佳实践、您应保留默认分数权重值、仅在需要时进行调整。

有关的参数和默认值的详细信息 `security dynamic-authorization trust-score-component modify` 命令、请参阅ONTAP手册页。

以下是您可以修改的组件及其默认分数和百分比权重：

标准	组件名称	默认原始分数权重	默认百分比权重
可信设备	`trusted-device`	20.	50.
用户登录身份验证历史记录	`authentication-history`	20.	50.

步骤

1. 修改信任得分组件。更新括号<>中的值以匹配您的环境。如果不使用 `-vserver` 参数、则命令将在集群级别运行。参数必须以粗体显示：

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

2. 查看得到的信任得分组件设置：

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

重置用户的信任得分

如果用户因系统策略而被拒绝访问、并且能够证明其身份、则管理员可以重置用户的信任得分。

有关的参数和默认值的详细信息 `security dynamic-authorization user-trust-score reset` 命令、请参阅ONTAP手册页。

步骤

1. 添加命令。请参见 [配置动态授权信任得分组件] 有关可重置的信任得分组件的列表。更新括号<>中的值以匹配您的环境。如果不使用 `-vserver` 参数、则命令将在集群级别运行。参数必须以粗体显示：

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

显示您的信任得分

用户可以显示其自己的登录会话信任得分。

步骤

1. 显示您的信任得分：

```
security login whoami
```

您应看到类似于以下内容的输出：

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

配置自定义信任得分提供程序

如果您已从外部信任得分提供程序收到评分方法、则可以将自定义提供程序添加到动态授权配置中。

开始之前

- 自定义信任得分提供程序必须返回JSON响应。必须满足以下语法要求：
  - 返回信任得分的字段必须是标量字段、而不是数组的元素。
  - 返回信任得分的字段可以是嵌套字段、例如 `trust_score.value`。
  - JSON响应中必须有一个字段返回数字信任得分。如果本机不可用、则可以编写包装程序脚本以返回此值。
- 提供的值可以是信任得分或风险得分。不同之处在于信任得分按升序排列、较高的分数表示较高的信任级别、而风险得分则按降序排列。例如、如果信任分数为90、分数范围为0到100、则表示该分数非常值得信

赖、并且可能会在不增加任何挑战的情况下获得"允许"、 如果分数范围为0到100、则风险分数为90表示风险较高、并且可能会在没有额外挑战的情况下导致"拒绝"。

- 自定义信任得分提供程序必须可通过ONTAP REST API进行访问。
- 必须使用支持的参数之一配置自定义信任得分提供程序。不支持需要在支持的参数列表中进行配置的自定义信任得分提供程序。

有关的参数和默认值的详细信息 `security dynamic-authorization trust-score-component create` 命令、请参阅ONTAP手册页。

步骤

1. 添加自定义信任得分提供程序。更新括号<>中的值以匹配您的环境。如果不使用 `-vserver` 参数、则命令将在集群级别运行。参数必须以粗体显示：

```
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. 查看得到的信任分数提供程序设置：

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

配置自定义信任得分提供程序标记

您可以使用标记与外部信任评分提供程序进行通信。这样、您就可以在不暴露敏感信息的情况下将URL中的信息发送到信任分数提供程序。

有关的参数和默认值的详细信息 `security dynamic-authorization trust-score-component create` 命令、请参阅ONTAP手册页。

步骤

1. 启用信任分数提供程序标记。更新括号<>中的值以匹配您的环境。如果不使用 `-vserver` 参数、则命令将在集群级别运行。参数必须以粗体显示：

```
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>
```

例如：

```
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"
```