



동적 권한 부여 관리

ONTAP 9

NetApp
June 19, 2024

목차

동적 권한 부여 관리	1
동적 인증 개요	1
동적 권한 부여를 사용하거나 사용하지 않습니다	1
동적 권한 부여를 사용자 지정합니다	3

동적 권한 부여 관리

동적 인증 개요

ONTAP 9.15.1부터 관리자는 동적 권한 부여를 구성 및 활성화하여 ONTAP에 대한 원격 액세스의 보안을 강화하는 한편 악의적인 행위자로 인해 발생할 수 있는 잠재적인 손상을 완화할 수 있습니다. ONTAP 9.15.1에서는 동적 권한 부여가 사용자에게 보안 점수를 할당하는 초기 프레임워크를 제공하며, 사용자의 활동이 의심스러운 경우 추가 권한 검사를 통해 사용자에게 문제를 주거나 작업을 완전히 거부할 수 있습니다. 관리자는 규칙을 만들고 신뢰 점수를 할당하며 제한 명령을 사용하여 특정 작업이 허용되거나 거부되는 시기를 결정할 수 있습니다. 관리자는 클러스터 전체 또는 개별 스토리지 VM에 대해 동적 권한 부여를 활성화할 수 있습니다.

동적 권한 부여 작동 방식

동적 권한 부여는 신뢰 점수 부여 시스템을 사용하여 권한 부여 정책에 따라 사용자에게 다른 신뢰 수준을 할당합니다. 사용자의 신뢰 수준에 따라 사용자가 수행하는 작업을 허용 또는 거부하거나 추가 인증을 요구하는 메시지가 표시될 수 있습니다.

불륨을 삭제하려고 하는 세 명의 다른 사용자의 예를 들어 보십시오. 작업을 수행하려고 할 때 각 사용자에게 대한 위험 등급이 검사됩니다.

- 첫 번째 사용자는 정규 업무 시간에 신뢰할 수 있는 장치에서 로그인하므로 위험 등급이 낮아지며 추가 인증 없이 작업이 허용됩니다.
- 두 번째 사용자는 업무 시간 외에 집에 있는 신뢰할 수 있는 장치에서 로그인하므로 위험 등급이 보통입니다. 작업을 허용하기 전에 추가 인증을 요청받습니다.
- 세 번째 사용자는 업무 시간 이외의 새 위치에서 신뢰할 수 없는 장치에서 로그인하므로 위험 등급이 높게 설정되고 작업이 허용되지 않습니다.

다음 단계

- "동적 권한 부여를 사용자 지정합니다"
- "동적 권한 부여를 사용하거나 사용하지 않습니다"

동적 권한 부여를 사용하거나 사용하지 않습니다

ONTAP 9.15.1부터 관리자는 에서 동적 권한 부여를 구성하고 활성화할 수 있습니다 visibility 모드 를 눌러 구성을 테스트하거나 에서 를 누릅니다 enforced SSH를 통해 접속하는 CLI 사용자에게 대한 구성을 활성화하는 모드입니다. 동적 인증이 더 이상 필요하지 않으면 비활성화할 수 있습니다. 동적 권한 부여를 비활성화해도 구성 설정을 계속 사용할 수 있으며 나중에 다시 사용하도록 설정하려는 경우 해당 설정을 사용할 수 있습니다.

의 매개 변수에 대한 자세한 내용은 를 참조하십시오 security dynamic-authorization modify ONTAP 설명서 페이지를 참조하십시오.

테스트에 대한 동적 인증을 활성화합니다

표시 모드에서 동적 권한 부여를 활성화하면 기능을 테스트하고 사용자가 실수로 잠기지 않도록 할 수 있습니다. 이 모드에서는 모든 제한된 작업에서 신뢰 점수가 확인되지만 적용되지는 않습니다. 그러나 거부되거나 추가 인증 문제가 발생했을 수 있는 모든 작업이 기록됩니다. 가장 좋은 방법은 의도한 설정을 적용하기 전에 이 모드에서 테스트해야 합니다.



다른 동적 권한 부여 설정을 아직 구성하지 않은 경우에도 이 단계에 따라 처음으로 동적 권한 부여를 활성화할 수 있습니다. 을 참조하십시오 ["동적 권한 부여를 사용자 지정합니다"](#) 기타 동적 권한 부여 설정을 사용자 환경에 맞게 구성하는 단계를 참조하십시오.

단계

1. 전역 설정을 구성하고 기능 상태를 로 변경하여 가시성 모드에서 동적 권한 부여를 활성화합니다 `visibility`. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

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

2. 를 사용하여 결과를 확인합니다 `show` 전역 설정을 표시하는 명령:

```
security dynamic-authorization show
```

강제 모드에서 동적 권한 부여를 활성화합니다

강제 적용 모드에서 동적 권한 부여를 활성화할 수 있습니다. 일반적으로 이 모드는 가시성 모드로 테스트를 완료한 후에 사용합니다. 이 모드에서는 모든 제한된 작업에서 신뢰 점수를 확인하고 제한 조건이 충족되면 활동 제한이 적용됩니다. 또한 억제 간격이 적용되어 지정된 간격 내에 추가적인 인증 문제가 발생하지 않습니다.



이 단계에서는 에서 동적 권한 부여를 이전에 구성하고 사용하도록 설정했다고 가정합니다 `visibility` 모드를 사용하는 것이 좋습니다.

단계

1. 에서 동적 권한 부여를 활성화합니다 `enforced` 모드로 변경합니다 `enforced`. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

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

2. 를 사용하여 결과를 확인합니다 show 전역 설정을 표시하는 명령:

```
security dynamic-authorization show
```

동적 권한 부여를 비활성화합니다

추가 인증 보안이 더 이상 필요하지 않은 경우 동적 권한 부여를 비활성화할 수 있습니다.

단계

1. 상태를 로 변경하여 동적 권한 부여를 비활성화합니다 disabled. 를 사용하지 않는 경우 -vserver 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

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

2. 를 사용하여 결과를 확인합니다 show 전역 설정을 표시하는 명령:

```
security dynamic-authorization show
```

다음 단계

(선택 사항) 환경에 따라 을 참조하십시오 "동적 권한 부여를 사용자 지정합니다" 기타 동적 권한 부여 설정을 구성합니다.

동적 권한 부여를 사용자 지정합니다

관리자는 동적 인증 구성의 다양한 측면을 사용자 지정하여 ONTAP 클러스터에 대한 원격 관리자 SSH 연결의 보안을 강화할 수 있습니다.

보안 요구에 따라 다음과 같은 동적 권한 부여 설정을 사용자 지정할 수 있습니다.

- 동적 권한 부여 전역 설정을 구성합니다
- 동적 권한 부여 신뢰 점수 구성 요소를 구성합니다
- 사용자 지정 신뢰 점수 공급자를 구성합니다
- 제한된 명령을 구성합니다
- 동적 권한 부여 그룹을 구성합니다

동적 권한 부여 전역 설정을 구성합니다

보호할 스토리지 VM, 인증 문제에 대한 억제 간격 및 신뢰 점수 설정을 비롯한 동적 권한 부여에 대한 글로벌 설정을 구성할 수 있습니다.

의 매개 변수 및 기본값에 대한 자세한 내용은 을 참조하십시오 `security dynamic-authorization modify` ONTAP 설명서 페이지를 참조하십시오.

단계

1. 동적 권한 부여에 대한 글로벌 설정을 구성합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다.

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

2. 결과 구성을 봅니다.

```
security dynamic-authorization show
```

제한된 명령을 구성합니다

동적 권한 부여를 사용하면 제한된 기본 명령 집합이 기능에 포함됩니다. 이 목록은 필요에 맞게 수정할 수 있습니다. 을 참조하십시오 "[MAV\(Multi-admin Verification\) 문서](#)" 제한된 명령의 기본 목록에 대한 자세한 내용은

제한된 명령을 추가합니다

동적 권한 부여로 제한된 명령 목록에 명령을 추가할 수 있습니다.

의 매개 변수 및 기본값에 대한 자세한 내용은 을 참조하십시오 `security dynamic-authorization rule create` ONTAP 설명서 페이지를 참조하십시오.

단계

1. 명령을 추가합니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

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

2. 제한된 명령의 결과 목록을 봅니다.

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

제한된 명령을 제거합니다

동적 권한 부여로 제한된 명령 목록에서 명령을 제거할 수 있습니다.

의 매개 변수 및 기본값에 대한 자세한 내용은 을 참조하십시오 security dynamic-authorization rule delete ONTAP 설명서 페이지를 참조하십시오.

단계

1. 명령을 제거합니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 -vserver 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

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

2. 제한된 명령의 결과 목록을 봅니다.

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

동적 권한 부여 그룹을 구성합니다

기본적으로 동적 권한 부여는 모든 사용자 및 그룹을 활성화하는 즉시 적용됩니다. 그러나 을 사용하여 그룹을 생성할 수 있습니다 security dynamic-authorization group create 명령을 사용하여 동적 권한이 특정 사용자에게만 적용되도록 합니다.

동적 권한 부여 그룹을 추가합니다

동적 권한 부여 그룹을 추가할 수 있습니다.

의 매개 변수 및 기본값에 대한 자세한 내용은 을 참조하십시오 security dynamic-authorization group create ONTAP 설명서 페이지를 참조하십시오.

단계

1. 그룹을 만듭니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 -vserver 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

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

2. 결과 동적 권한 부여 그룹을 봅니다.

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

동적 권한 부여 그룹을 제거합니다

동적 권한 부여 그룹을 제거할 수 있습니다.

단계

1. 그룹을 삭제합니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

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

2. 결과 동적 권한 부여 그룹을 봅니다.

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

동적 권한 부여 신뢰 점수 구성 요소를 구성합니다

점수 매기기 기준의 우선 순위를 변경하거나 위험 점수에서 특정 기준을 제거하도록 최대 점수 가중치를 구성할 수 있습니다.



가장 좋은 방법은 기본 점수 가중치를 그대로 두고 필요한 경우에만 조정해야 합니다.

의 매개 변수 및 기본값에 대한 자세한 내용은 을 참조하십시오 `security dynamic-authorization trust-score-component modify` ONTAP 설명서 페이지를 참조하십시오.

다음은 기본 점수 및 백분율 가중치와 함께 수정할 수 있는 구성 요소입니다.

기준	부품 이름	기본 원시 점수 가중치	기본 백분율 가중치
신뢰할 수 있는 장치	trusted-device	20	50
사용자 로그인 인증 기록	authentication-history	20	50

단계

1. 신뢰 점수 구성 요소를 수정합니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

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

2. 결과 신뢰 점수 구성 요소 설정을 봅니다.

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

사용자의 신뢰 점수를 재설정합니다

시스템 정책으로 인해 사용자의 액세스가 거부되고 ID를 입증할 수 있는 경우 관리자는 사용자의 신뢰 점수를 재설정할 수 있습니다.

의 매개 변수 및 기본값에 대한 자세한 내용은 을 참조하십시오 `security dynamic-authorization user-trust-score reset` ONTAP 설명서 페이지를 참조하십시오.

단계

1. 명령을 추가합니다. 을 참조하십시오 [동적 권한 부여 신뢰 점수 구성 요소를 구성합니다](#) 재설정할 수 있는 신뢰 점수 구성 요소 목록 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

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

신뢰 점수를 표시합니다

사용자는 로그인 세션에 대해 자신의 신뢰 점수를 표시할 수 있습니다.

단계

1. 신뢰 점수 표시:

```
security login whoami
```

다음과 유사한 출력이 표시됩니다.

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

사용자 지정 신뢰 점수 공급자를 구성합니다

외부 신뢰 점수 공급자로부터 채점 방법을 이미 받은 경우 사용자 지정 공급자를 동적 권한 부여 구성에 추가할 수 있습니다.

시작하기 전에

- 사용자 지정 신뢰 점수 공급자는 JSON 응답을 반환해야 합니다. 다음 구문 요구 사항을 충족해야 합니다.
 - 신뢰 점수를 반환하는 필드는 스칼라 필드여야 하며 배열 요소가 아닙니다.
 - 신뢰 점수를 반환하는 필드는 과 같이 중첩된 필드가 될 수 있습니다 `trust_score.value`.
 - JSON 응답 내에 숫자 신뢰 점수를 반환하는 필드가 있어야 합니다. 이 값을 기본적으로 사용할 수 없는 경우 래퍼 스크립트를 작성하여 이 값을 반환할 수 있습니다.
- 제공된 값은 신뢰 점수 또는 위험 점수일 수 있습니다. 신뢰 점수는 오름차순이고 신뢰 수준이 높을수록 높은 반면 위험 점수는 내림차순이라는 차이가 있습니다. 예를 들어 0에서 100 사이의 점수 범위에 대해 신뢰 점수가 90이면 점수가 매우 신뢰할 수 있고 추가 도전 없이 "허용"이 될 가능성이 높다는 것을 나타냅니다. 점수 범위가 0 ~ 100인 경우 위험 점수가 90이면 고위험이며 추가 도전 없이 "거부"가 발생할 가능성이 높습니다.
- ONTAP REST API를 통해 사용자 지정 신뢰 점수 공급자에 액세스할 수 있어야 합니다.
- 사용자 지정 신뢰 점수 공급자는 지원되는 매개 변수 중 하나를 사용하여 구성할 수 있어야 합니다. 지원되는 매개 변수 목록에 없는 구성이 필요한 사용자 지정 신뢰 점수 공급자는 지원되지 않습니다.

의 매개 변수 및 기본값에 대한 자세한 내용은 을 참조하십시오 `security dynamic-authorization trust-score-component create` ONTAP 설명서 페이지를 참조하십시오.

단계

1. 사용자 지정 신뢰 점수 공급자를 추가합니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 `-vserver` 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

```
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. 결과 신뢰 점수 공급자 설정을 봅니다.

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

사용자 지정 신뢰 점수 공급자 태그를 구성합니다

태그를 사용하여 외부 신뢰 점수 공급자와 통신할 수 있습니다. 이렇게 하면 중요한 정보를 노출하지 않고 URL의 정보를 신뢰 점수 공급자로 보낼 수 있습니다.

의 매개 변수 및 기본값에 대한 자세한 내용은 을 참조하십시오 security dynamic-authorization trust-score-component create ONTAP 설명서 페이지를 참조하십시오.

단계

1. 신뢰 점수 공급자 태그를 활성화합니다. 괄호(>)의 값을 환경에 맞게 업데이트합니다. 를 사용하지 않는 경우 -vserver 매개 변수로, 명령은 클러스터 레벨에서 실행됩니다. 굵은 글씨로 표시된 매개 변수가 필요합니다.

```
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>
```

예를 들면 다음과 같습니다.

```
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"
```

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.