CLI를 사용하여 클러스터에 액세스(클러스터 관리자만 해당)

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/ontap/system-admin/access-serial-port-task.html on April 24, 2024. Always check docs.netapp.com for the latest.

목차

CLI를 사용하여 클러스터에 액세스(클러스터 관리자만 해당)

직렬 포트를 사용하여 클러스터에 액세스합니다

노드의 시리얼 포트에 연결된 콘솔에서 클러스터에 직접 액세스할 수 있습니다.

단계

1. 콘솔에서 Enter 키를 누릅니다.

   시스템이 로그인 프롬프트로 응답합니다.

2. 로그인 프롬프트에서 다음 중 하나를 수행합니다.

를 사용하여 클러스터에 액세스하는 방법	다음 계정 이름을 입력하십시오...
기본 클러스터 계정입니다	' * admin * '
대체 관리 사용자 계정입니다	'*username*'

   시스템이 암호 프롬프트로 응답합니다.

3. admin 또는 administrative 사용자 계정의 암호를 입력한 다음 Enter 키를 누릅니다.

SSH를 사용하여 클러스터에 액세스합니다

클러스터에 SSH 요청을 실행하여 관리 작업을 수행할 수 있습니다. SSH는 기본적으로 사용하도록 설정됩니다.

필요한 것

- 'sh'를 액세스 방법으로 사용하도록 구성된 사용자 계정이 있어야 합니다.

  를 클릭합니다 `-application` 의 매개 변수입니다 `security login` 명령은 사용자 계정에 대한 액세스 방법을 지정합니다. 를 클릭합니다 `security login` "Man 페이지" 추가 정보를 포함합니다.

- AD(Active Directory) 도메인 사용자 계정을 사용하여 클러스터에 액세스하는 경우 CIFS 지원 스토리지 VM을 통해 클러스터에 대한 인증 터널을 설정해야 하며 AD 도메인 사용자 계정도 를 사용하여 클러스터에 추가되어야 합니다 `ssh` 액세스 방법 및 로 `domain` 인증 방법으로 사용합니다.
- IPv6 연결을 사용하는 경우 IPv6가 이미 클러스터에서 구성 및 활성화되어 있어야 하며, 방화벽 정책이 이미 IPv6 주소로 구성되어 있어야 합니다.

  network options ipv6 show 명령을 실행하면 IPv6의 활성화 여부가 표시됩니다. 'system services firewall policy show' 명령은 방화벽 정책을 표시합니다.

이 작업에 대해

- OpenSSH 5.7 이상 클라이언트를 사용해야 합니다.
- SSH v2 프로토콜만 지원되며 SSH v1은 지원되지 않습니다.
- ONTAP는 노드당 최대 64개의 동시 SSH 세션을 지원합니다.

  클러스터 관리 LIF가 노드에 상주하는 경우 이 제한을 노드 관리 LIF와 공유합니다.

  들어오는 연결의 비율이 초당 10보다 높을 경우 서비스가 60초 동안 일시적으로 비활성화됩니다.

- ONTAP는 SSH에 대해 AES 및 3DES 암호화 알고리즘(_ciphers _ 라고도 함)만 지원합니다.

  AES는 키 길이가 128, 192 및 256비트인 경우 지원됩니다. 3DES는 원래 DES와 마찬가지로 키 길이가 56비트이지만 세 번 반복됩니다.

- FIPS 모드가 켜져 있는 경우 SSH 클라이언트는 연결이 성공할 수 있도록 Elliptic Curve Digital Signature Algorithm(ECDSA) 공개 키 알고리즘과 협상해야 합니다.
- Windows 호스트에서 ONTAP CLI에 액세스하려는 경우 PuTTY와 같은 타사 유틸리티를 사용할 수 있습니다.
- Windows AD 사용자 이름을 사용하여 ONTAP에 로그인하는 경우 ONTAP에서 AD 사용자 이름과 도메인 이름을 만들 때 사용한 대문자나 소문자를 동일하게 사용해야 합니다.

  AD 사용자 이름과 도메인 이름은 대소문자를 구분하지 않습니다. 그러나 ONTAP 사용자 이름은 대/소문자를 구분합니다. ONTAP에서 생성된 사용자 이름과 AD에서 생성된 사용자 이름 간의 케이스 불일치로 인해 로그인 오류가 발생합니다.

SSH 인증 옵션

- ONTAP 9.3부터 가능합니다 "SSH 다단계 인증 지원" 로컬 관리자 계정의 경우.

  SSH 다단계 인증을 사용하면 공개 키와 암호를 사용하여 사용자를 인증할 수 있습니다.

- ONTAP 9.4부터 가능합니다 "SSH 다단계 인증 지원" LDAP 및 NIS 원격 사용자의 경우
- ONTAP 9.13.1 부터는 선택적으로 SSH 인증 프로세스에 인증서 유효성 검사를 추가하여 로그인 보안을 강화할 수 있습니다. 이렇게 하려면 "X.509 인증서를 공개 키와 연결합니다" 계정이 사용하는 것입니다. SSH 공개 키와 X.509 인증서를 모두 사용하여 SSH에 로그인하는 경우 ONTAP는 SSH 공개 키로 인증하기 전에 X.509 인증서의 유효성을 검사합니다. 인증서가 만료되거나 해지되고 SSH 공개 키가 자동으로 비활성화되면 SSH 로그인이 거부됩니다.
- ONTAP 9.14.1부터 선택적으로 Cisco Duo 2단계 인증을 SSH 인증 프로세스에 추가하여 로그인 보안을 강화할 수 있습니다. Cisco Duo 인증을 활성화한 후 처음 로그인할 때 사용자는 SSH 세션에 대한 인증자로 사용할 장치를 등록해야 합니다. 을 참조하십시오 "SSH 로그인에 Cisco Duo 2FA를 구성합니다" ONTAP용 Cisco Duo SSH 인증 구성에 대한 자세한 내용은

단계

1. 관리 호스트에서 'sh' 명령을 다음 형식 중 하나로 입력합니다.
   - '* ssh_username@hostname_or_ip_[*command*] *'
   - '* ssh-l_username hostname_or_ip_[*command*] * '

AD 도메인 사용자 계정을 사용하는 경우 '*username*'을 '*domainname\\AD_accountname*'(도메인 이름 뒤에 이중 백슬래시를 사용하여) 또는 '"*domainname\AD_accountname*"'(큰따옴표로 묶고 도메인 이름 뒤에 백슬래시를 하나씩 붙여야 합니다) 형식으로 지정해야 합니다.

'*hostname_or_ip*'은 클러스터 관리 LIF 또는 노드 관리 LIF의 호스트 이름 또는 IP 주소입니다. 클러스터 관리 LIF를 사용하는 것이 좋습니다. IPv4 또는 IPv6 주소를 사용할 수 있습니다.

SSH-Interactive 세션에는 '*command*'가 필요하지 않습니다.

SSH 요청의 예

다음 예에서는 사용자 계정 ""Joe""가 클러스터 관리 LIF가 10.72.137.28인 클러스터에 액세스하는 SSH 요청을 발행하는 방법을 보여줍니다.

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

다음 예에서는 "DOMAIN1" 도메인의 사용자 계정 ""John""이 클러스터 관리 LIF가 10.72.137.28인 클러스터에 액세스하기 위한 SSH 요청을 실행할 수 있는 방법을 보여줍니다.

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

다음 예에서는 사용자 계정 ""Joe""가 클러스터 관리 LIF가 10.72.137.32인 클러스터에 액세스하는 SSH MFA 요청을 발행하는 방법을 보여줍니다.

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

관련 정보

"관리자 인증 및 RBAC"

SSH 로그인 보안

ONTAP 9.5부터 이전 로그인에 대한 정보, 로그인 시도 실패 및 마지막으로 성공한 로그인 이후 권한 변경 내용을 볼 수 있습니다.

SSH admin 사용자로 로그인하면 보안 관련 정보가 표시됩니다. 다음 조건에 대한 경고가 표시됩니다.

- 계정 이름이 마지막으로 로그인한 시간입니다.
- 마지막으로 성공한 로그인 이후 실패한 로그인 시도 횟수입니다.
- 마지막 로그인 이후 역할이 변경되었는지 여부(예: admin 계정의 역할이 "admin"에서 "backup"으로 변경된 경우)
- 마지막 로그인 이후 역할의 추가, 수정 또는 삭제 기능이 수정되었는지 여부

표시된 정보가 의심스러운 경우 즉시 보안 부서에 문의해야 합니다.

로그인할 때 이 정보를 얻으려면 다음 필수 구성 요소가 충족되어야 합니다.

- ONTAP에서 SSH 사용자 계정을 프로비저닝해야 합니다.
- SSH 보안 로그인을 생성해야 합니다.

- 로그인 시도가 성공해야 합니다.

SSH 로그인 보안에 대한 제한 및 기타 고려 사항

SSH 로그인 보안 정보에는 다음과 같은 제한 및 고려 사항이 적용됩니다.

- 이 정보는 SSH 기반 로그인에만 사용할 수 있습니다.
- LDAP/NIS 및 AD 계정과 같은 그룹 기반 관리자 계정의 경우, 사용자는 자신이 속한 그룹이 ONTAP에서 관리자 계정으로 할당된 경우 SSH 로그인 정보를 볼 수 있습니다.

  그러나 이러한 사용자에 대해서는 사용자 계정의 역할 변경에 대한 알림을 표시할 수 없습니다. 또한 ONTAP에서 admin 계정으로 프로비저닝된 AD 그룹에 속한 사용자는 마지막으로 로그인한 이후 실패한 로그인 시도 횟수를 볼 수 없습니다.

- ONTAP에서 사용자 계정을 삭제하면 해당 사용자에 대해 유지되는 정보가 삭제됩니다.
- SSH가 아닌 애플리케이션 접속에 대한 정보는 표시되지 않습니다.

SSH 로그인 보안 정보의 예

다음 예에서는 로그인 후 표시되는 정보의 유형을 보여 줍니다.

- 이 메시지는 로그인에 성공할 때마다 표시됩니다.

```
Last Login : 7/19/2018 06:11:32
```

- 마지막으로 성공한 로그인 이후 로그인 시도가 실패한 경우 다음 메시지가 표시됩니다.

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- 로그인 시도 실패 및 마지막 로그인 후 권한이 수정된 경우 다음 메시지가 표시됩니다.

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

클러스터에 대한 Telnet 또는 RSH 액세스를 활성화합니다

최선의 보안 방법으로, Telnet과 RSH는 미리 정의된 관리 방화벽 정책(mGMT)에서 비활성화됩니다. 클러스터가 텔넷 또는 RSH 요청을 수락하도록 설정하려면 텔넷 또는 RSH가 설정된 새 관리 방화벽 정책을 생성한 다음 새 정책을 클러스터 관리 LIF와 연결해야 합니다.

이 작업에 대해

ONTAP는 미리 정의된 방화벽 정책을 변경하지 못하도록 하지만 미리 정의된 "GMT" 관리 방화벽 정책을 복제한 다음 새 정책에서 텔넷 또는 RSH를 활성화하여 새 정책을 만들 수 있습니다. 그러나 Telnet과 RSH는 보안 프로토콜이 아니므로 SSH를 사용하여 클러스터에 액세스하는 것을 고려해야 합니다. SSH는 보안 원격 셸 및 대화형 네트워크 세션을 제공합니다.

클러스터에 대한 텔넷 또는 RSH 액세스를 활성화하려면 다음 단계를 수행하십시오.

단계

1. 고급 권한 모드(* SET ADVANCED *)로 진입합니다
2. 보안 프로토콜(RSH 또는 TELNET) 사용: (* security protocol modify -application_security_protocol_-enabled true*)
3. mGMT 관리 방화벽 정책, 즉 `* 시스템 서비스 방화벽 정책 클론-정책 관리-대상-정책_정책-이름_*'을 기반으로 새 관리 방화벽 정책을 만듭니다
4. 새 관리 방화벽 정책에서 텔넷 또는 RSH를 활성화합니다. (* 시스템 서비스 방화벽 정책 create-policy_name_-service_security_protocol_-action allow-ip-list_ip_address/netmask_*) 모든 IP 주소를 허용하려면 '-ip-list 0.0.0.0/0'을 지정해야 합니다
5. 새 정책을 클러스터 관리 LIF: `* 네트워크 인터페이스 수정 -vserver_cluster_management_LIF_-lif cluster_mgmt -firewall_policy_name_ * '과(와) 연계합니다

텔넷을 사용하여 클러스터에 액세스합니다

클러스터에 텔넷 요청을 실행하여 관리 작업을 수행할 수 있습니다. 텔넷은 기본적으로 비활성화되어 있습니다.

필요한 것

텔넷을 사용하여 클러스터에 액세스하려면 다음 조건이 충족되어야 합니다.

- 텔넷을 액세스 방법으로 사용하도록 구성된 클러스터 로컬 사용자 계정이 있어야 합니다.

  '보안 로그인' 명령어의 '-application' 파라미터는 사용자 계정에 대한 접속 방식을 지정한다. 자세한 내용은 보안 로그인 man 페이지를 참조하십시오.

- Telnet 요청이 방화벽을 통과할 수 있도록 클러스터나 노드 관리 LIF에서 사용하는 관리 방화벽 정책에서 텔넷이 이미 활성화되어 있어야 합니다.

  기본적으로 텔넷은 비활성화되어 있습니다. 시스템 서비스 방화벽 정책 show 명령을 -service telnet 매개변수와 함께 실행하면 텔넷이 방화벽 정책에서 활성화되었는지의 여부가 표시됩니다. 자세한 내용은 시스템 서비스 방화벽 정책 man 페이지를 참조하십시오.

- IPv6 연결을 사용하는 경우 IPv6가 이미 클러스터에서 구성 및 활성화되어 있어야 하며, 방화벽 정책이 이미 IPv6 주소로 구성되어 있어야 합니다.

  network options ipv6 show 명령을 실행하면 IPv6의 활성화 여부가 표시됩니다. 'system services firewall policy show' 명령은 방화벽 정책을 표시합니다.

이 작업에 대해

- 텔넷은 보안 프로토콜이 아닙니다.

SSH를 사용하여 클러스터에 액세스하는 것을 고려해야 합니다. SSH는 보안 원격 셸 및 대화형 네트워크 세션을 제공합니다.

- ONTAP는 노드당 최대 50개의 동시 텔넷 세션을 지원합니다.

  클러스터 관리 LIF가 노드에 상주하는 경우 이 제한을 노드 관리 LIF와 공유합니다.

  들어오는 연결의 비율이 초당 10보다 높을 경우 서비스가 60초 동안 일시적으로 비활성화됩니다.

- Windows 호스트에서 ONTAP CLI에 액세스하려는 경우 PuTTY와 같은 타사 유틸리티를 사용할 수 있습니다.

단계

1. 관리 호스트에서 다음 명령을 입력합니다.

   '* telnet_hostname_or_ip_ * '

   '*hostname_or_ip*'은 클러스터 관리 LIF 또는 노드 관리 LIF의 호스트 이름 또는 IP 주소입니다. 클러스터 관리 LIF를 사용하는 것이 좋습니다. IPv4 또는 IPv6 주소를 사용할 수 있습니다.

텔넷 요청의 예

다음 예에서는 텔넷 액세스를 사용하여 설정된 ""Joe""라는 사용자가 클러스터 관리 LIF가 10.72.137.28인 클러스터에 액세스하기 위한 텔넷 요청을 실행할 수 있는 방법을 보여줍니다.

```
admin_host$ telnet 10.72.137.28
Data ONTAP
login: joe
Password:
cluster1::>
```

RSH를 사용하여 클러스터에 액세스합니다

RSH 요청을 클러스터에 발행하여 관리 작업을 수행할 수 있습니다. RSH는 보안 프로토콜이 아니며 기본적으로 비활성화되어 있습니다.

필요한 것

RSH를 사용하여 클러스터에 액세스하려면 다음 조건을 충족해야 합니다.

- RSH를 액세스 방법으로 사용하도록 구성된 클러스터 로컬 사용자 계정이 있어야 합니다.

  '보안 로그인' 명령어의 '-application' 파라미터는 사용자 계정에 대한 접속 방식을 지정한다. 자세한 내용은 보안 로그인 man 페이지를 참조하십시오.

- RSH 요청이 방화벽을 통과할 수 있도록 클러스터 또는 노드 관리 LIF에서 사용하는 관리 방화벽 정책에서 RSH가 이미 활성화되어 있어야 합니다.

  기본적으로 RSH는 비활성화되어 있습니다. system services firewall policy show 명령을 `-service rsh' 매개변수와 함께 사용하면 방화벽 정책에서 RSH가 활성화되었는지 여부가 표시됩니다. 자세한 내용은 시스템 서비스 방화벽 정책 man 페이지를 참조하십시오.

- IPv6 연결을 사용하는 경우 IPv6가 이미 클러스터에서 구성 및 활성화되어 있어야 하며, 방화벽 정책이 이미 IPv6 주소로 구성되어 있어야 합니다.

  network options ipv6 show 명령을 실행하면 IPv6의 활성화 여부가 표시됩니다. 'system services firewall policy show' 명령은 방화벽 정책을 표시합니다.

이 작업에 대해

- RSH는 보안 프로토콜이 아닙니다.

  SSH를 사용하여 클러스터에 액세스하는 것을 고려해야 합니다. SSH는 보안 원격 셸 및 대화형 네트워크 세션을 제공합니다.

- ONTAP는 노드당 최대 50개의 동시 RSH 세션을 지원한다.

  클러스터 관리 LIF가 노드에 상주하는 경우 이 제한을 노드 관리 LIF와 공유합니다.

  들어오는 연결의 비율이 초당 10보다 높을 경우 서비스가 60초 동안 일시적으로 비활성화됩니다.

단계

1. 관리 호스트에서 다음 명령을 입력합니다.

   '* rsh_hostname_or_ip_-l_username:passwordcommand_ *'

   '*hostname_or_ip*'은 클러스터 관리 LIF 또는 노드 관리 LIF의 호스트 이름 또는 IP 주소입니다. 클러스터 관리 LIF를 사용하는 것이 좋습니다. IPv4 또는 IPv6 주소를 사용할 수 있습니다.

   '*command*'는 RSH를 통해 실행하려는 명령입니다.

RSH 요청의 예

다음 예에서는 RSH 액세스를 사용하여 설정된 ""Joe""라는 사용자가 "cluster show" 명령을 실행하도록 RSH 요청을 실행하는 방법을 보여줍니다.

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

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 라이센스와 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 라이센스도 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 라이센스를 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 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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