구축 후 **SolidFire** 시스템 옵션을 구성합니다

Element Software

NetApp
October 01, 2024

목차

구축 후 SolidFire 시스템 옵션을 구성합니다

SolidFire 시스템을 설정한 후 몇 가지 선택적 작업을 수행할 수 있습니다.

시스템에서 자격 증명을 변경하는 경우 다른 구성 요소에 미치는 영향을 알고 싶을 수 있습니다.

또한 다중 요소 인증, 외부 키 관리 및 FIPS(Federal Information Processing Standards) 보안에 대한 설정을 구성할 수 있습니다. 필요한 경우 암호 업데이트도 고려해야 합니다.

자세한 내용을 확인하십시오

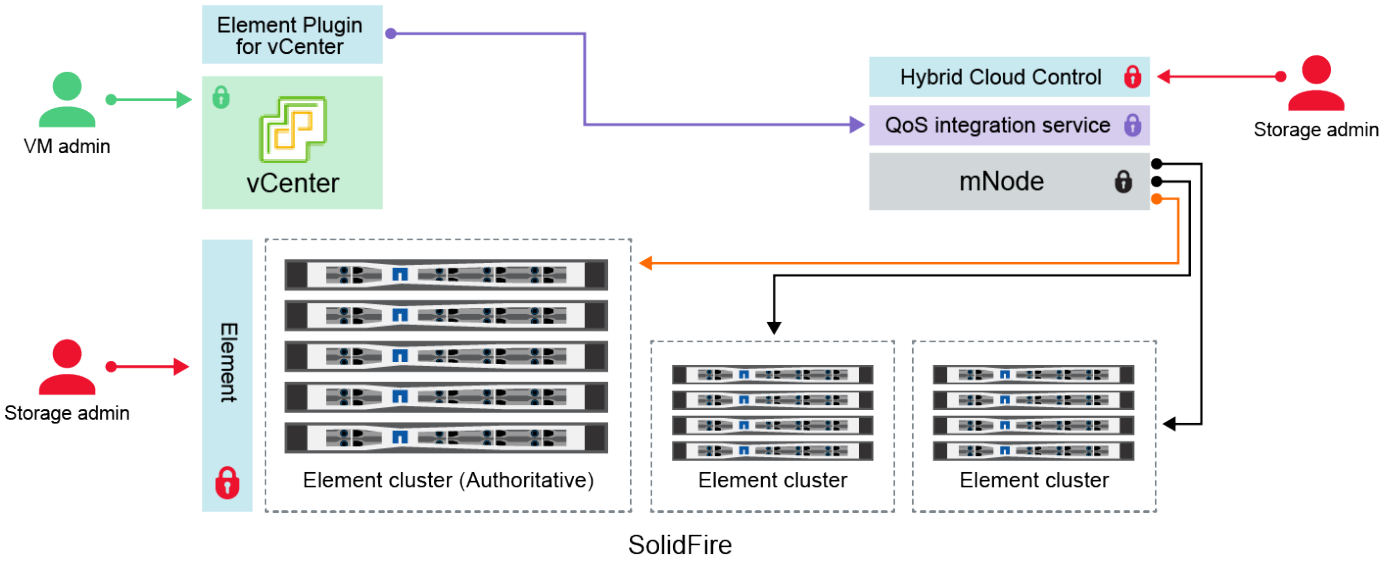
- "NetApp HCI 및 NetApp SolidFire에서 자격 증명을 변경합니다"
- "Element 소프트웨어 기본 SSL 인증서를 변경합니다"
- "노드의 IPMI 암호를 변경합니다"
- "다중 요소 인증을 사용합니다"
- "외부 키 관리를 시작합니다"
- "FIPS 드라이브를 지원하는 클러스터를 생성합니다"

NetApp HCI 및 NetApp SolidFire에서 자격 증명을 변경합니다

NetApp HCI 또는 NetApp SolidFire를 구축한 조직의 보안 정책에 따라 자격 증명 또는 암호를 변경하는 것이 일반적으로 보안 사례의 일부입니다. 암호를 변경하기 전에 배포의 다른 소프트웨어 구성 요소에 미치는 영향을 알고 있어야 합니다.

NetApp HCI 또는 NetApp SolidFire 구축의 구성 요소 중 하나에 대한 자격 증명을 변경하는 경우 다음 표에서는 다른 구성 요소에 미치는 영향에 대한 지침을 제공합니다.

NetApp SolidFire 구성 요소 상호 작용:



자격 증명 유형 및 아이콘	관리자별 사용	이 지침을 참조하십시오
요소 자격 증명 	• 는 *:NetApp HCI 및 SolidFire에 적용됩니다 관리자는 다음 자격 증명을 사용하여 에 로그인합니다. • Element 스토리지 클러스터의 요소 사용자 인터페이스 • 관리 노드에서의 하이브리드 클라우드 제어(mnode) Hybrid Cloud Control은 여러 스토리지 클러스터를 관리할 때 mnode가 처음에 설정한 _authoritative cluster_로 알려진 스토리지 클러스터에 대한 관리자 자격 증명만 수락합니다. 나중에 하이브리드 클라우드 제어에 추가된 스토리지 클러스터의 경우 mnode는 관리자 자격 증명을 안전하게 저장합니다. 이후에 추가된 스토리지 클러스터에 대한 자격 증명이 변경된 경우 mnode API를 사용하여 mnode에서도 자격 증명을 업데이트해야 합니다.	• "스토리지 클러스터 관리자 암호를 업데이트합니다." • 를 사용하여 mnode에서 스토리지 클러스터 관리자 자격 증명을 "modifyclusteradmin API를 사용합니다"업데이트합니다.

자격 증명 유형 및 아이콘	관리자별 사용	이 지침을 참조하십시오
vSphere SSO(Single Sign-On) 자격 증명 	• 는 *:NetApp HCI에만 적용됩니다 관리자는 이러한 자격 증명을 사용하여 VMware vSphere Client에 로그인합니다. vCenter가 NetApp HCI 설치의 일부인 경우 자격 증명은 다음과 같이 NetApp 배포 엔진에서 구성됩니다. • username@vsphere.loca l 에 지정된 암호 및 를 입력합니다 • administrator@vsphere.loca l 을 입력합니다. 기존 vCenter를 사용하여 NetApp HCI를 구축하면 IT VMware 관리자가 vSphere Single Sign-On 자격 증명을 관리합니다.	"vCenter 및 ESXi 자격 증명을 업데이트합니다"..
베이스보드 관리 컨트롤러(BMC) 자격 증명 	• 는 *:NetApp HCI에만 적용됩니다 관리자는 이러한 자격 증명을 사용하여 NetApp HCI 배포에서 NetApp 컴퓨팅 노드의 BMC에 로그인합니다. BMC는 기본 하드웨어 모니터링 및 가상 콘솔 기능을 제공합니다. 각 NetApp 컴퓨팅 노드에 대한 BMC(*IPMI* 라고도 함) 자격 증명은 NetApp HCI 배포의 mnode에 안전하게 저장됩니다. NetApp 하이브리드 클라우드 제어에서는 서비스 계정 용량의 BMC 자격 증명을 사용하여 컴퓨팅 노드 펌웨어 업그레이드 중에 컴퓨팅 노드의 BMC와 통신합니다. BMC 자격 증명이 변경되면 해당 컴퓨팅 노드의 자격 증명이 mnode에서도 업데이트되어야 모든 하이브리드 클라우드 제어 기능을 유지할 수 있습니다.	• "NetApp HCI의 각 노드에 대해 IPMI를 구성합니다".. • H410C, H610C 및 H615C 노드의 경우,"기본 IPMI 암호를 변경합니다" • H410S 및 H610S 노드의 "기본 IPM 암호를 변경합니다"경우, • "관리 노드에서 BMC 자격 증명을 변경합니다"..
ESXi 자격 증명 	• 는 *:NetApp HCI에만 적용됩니다 관리자는 SSH 또는 로컬 루트 계정이 있는 로컬 DCUI를 사용하여 ESXi 호스트에 로그인할 수 있습니다. NetApp HCI 배포에서는 사용자 이름이 '루트'이고 NetApp 배포 엔진에서 해당 컴퓨팅 노드를 처음 설치할 때 암호를 지정했습니다. 각 NetApp 컴퓨팅 노드의 ESXi 루트 자격 증명은 NetApp HCI 구축의 mnode에 안전하게 저장됩니다. NetApp 하이브리드 클라우드 제어에서는 서비스 계정 용량의 자격 증명을 사용하여 컴퓨팅 노드 펌웨어 업그레이드 및 상태 점검 중에 ESXi 호스트와 직접 통신합니다. VMware 관리자가 ESXi 루트 자격 증명을 변경하면 하이브리드 클라우드 제어 기능을 유지하려면 해당 컴퓨팅 노드의 자격 증명을 mnode에서 업데이트해야 합니다.	"vCenter 및 ESXi 호스트에 대한 자격 증명을 업데이트합니다"..

자격 증명 유형 및 아이콘	관리자별 사용	이 지침을 참조하십시오
QoS 통합 암호입니다 	• 는 *:NetApp HCI에 적용되며 SolidFire에서는 선택 사항입니다 관리자의 대화형 로그인에는 사용되지 않습니다. VMware vSphere와 Element 소프트웨어 간의 QoS 통합은 다음을 통해 활성화됩니다. • vCenter Server용 Element 플러그인 및 입니다 • mnode의 QoS 서비스. 인증을 위해 QoS 서비스는 이 컨텍스트에서만 사용되는 암호를 사용합니다. QoS 암호는 vCenter Server용 Element 플러그인을 처음 설치하는 동안 또는 NetApp HCI 구축 중에 자동으로 생성되는 동안 지정됩니다. 다른 구성 요소에 영향을 주지 않습니다.	"vCenter Server용 NetApp Element 플러그인에서 QoSSIOC 자격 증명을 업데이트합니다".. vCenter Server SIOC용 NetApp Element 플러그인은 _ QoSSIOC 암호 _ 라고도 합니다. https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Element_Plug-in_for_vCenter_server/mNode_Status_shows_as_'Network_Down'_or_'Down'_in_the_mNode_Settings_tab_of_the_Element_Plugin_for_vCenter_(VCP) [vCenter Server용 Element Plug-in KB 문서^]를 검토합니다.
vCenter Service Applianc e 자격 증명 	• 는 NetApp 배포 엔진에서 설정한 경우에만 *:NetApp HCI에 적용됩니다 관리자는 vCenter Server 어플라이언스 가상 머신에 로그인할 수 있습니다. NetApp HCI 배포에서는 사용자 이름이 '루트'이고 NetApp 배포 엔진에서 해당 컴퓨팅 노드를 처음 설치할 때 암호를 지정했습니다. 구축된 VMware vSphere 버전에 따라 vSphere Single Sign-On 도메인의 특정 관리자도 어플라이언스에 로그인할 수 있습니다. 다른 구성 요소에 영향을 주지 않습니다.	변경할 필요가 없습니다.
NetApp 관리 노드 관리자 자격 증명 	• 는 *:NetApp HCI에 적용되며 SolidFire에서는 선택 사항입니다 관리자는 NetApp 관리 노드 가상 머신에 로그인하여 고급 구성 및 문제 해결을 수행할 수 있습니다. 구축된 관리 노드 버전에 따라 SSH를 통한 로그인은 기본적으로 사용되지 않습니다. NetApp HCI 배포에서는 NetApp 배포 엔진에서 해당 컴퓨팅 노드를 처음 설치할 때 사용자가 사용자 이름과 암호를 지정했습니다. 다른 구성 요소에 영향을 주지 않습니다.	변경할 필요가 없습니다.

자세한 내용을 확인하십시오

- "Element 소프트웨어 기본 SSL 인증서를 변경합니다"
- "노드의 IPMI 암호를 변경합니다"
- "다중 요소 인증을 사용합니다"
- "외부 키 관리를 시작합니다"
- "FIPS 드라이브를 지원하는 클러스터를 생성합니다"

Element 소프트웨어 기본 SSL 인증서를 변경합니다

NetApp Element API를 사용하여 클러스터에 있는 스토리지 노드의 기본 SSL 인증서 및 개인 키를 변경할 수 있습니다.

NetApp Element 소프트웨어 클러스터가 생성되면 클러스터는 Element UI, Per-Node UI 또는 API를 통해 모든 HTTPS 통신에 사용되는 고유한 자체 서명된 SSL(Secure Sockets Layer) 인증서와 개인 키를 생성합니다. Element 소프트웨어는 자체 서명된 인증서뿐만 아니라 신뢰할 수 있는 CA(인증 기관)에서 발급 및 확인되는 인증서도 지원합니다.

다음 API 메소드를 사용하여 기본 SSL 인증서에 대한 자세한 정보를 얻고 변경할 수 있습니다.

- * GetSSLCertificate *

  를 사용하여 모든 인증서 세부 정보를 포함하여 현재 설치된 SSL 인증서에 대한 정보를 검색할 수 "GetSSLCertificate 메서드"있습니다.

- * SetSSLCertificate *

  를 사용하여 클러스터 및 노드별 SSL 인증서를 사용자가 제공하는 인증서 및 개인 키로 설정할 수 "SetSSLCertificate 메서드"있습니다. 시스템은 유효하지 않은 인증서가 적용되지 않도록 인증서와 개인 키의 유효성을 검사합니다.

- * RemoveSSLCertificate * 를 선택합니다

  는 "RemoveSSLCertificate 메서드입니다"현재 설치된 SSL 인증서 및 개인 키를 제거합니다. 그런 다음 클러스터가 새로운 자체 서명된 인증서와 개인 키를 생성합니다.

> ⓘ 클러스터 SSL 인증서는 클러스터에 추가된 모든 새 노드에 자동으로 적용됩니다. 클러스터에서 제거된 노드는 자체 서명된 인증서로 되돌리며 모든 사용자 정의 인증서와 키 정보가 노드에서 제거됩니다.

자세한 내용을 확인하십시오

- "관리 노드의 기본 SSL 인증서를 변경합니다"
- "Element 소프트웨어에서 사용자 정의 SSL 인증서를 설정하는 데 필요한 요구 사항은 무엇입니까?"
- "SolidFire 및 Element 소프트웨어 설명서"
- "vCenter Server용 NetApp Element 플러그인"

노드의 기본 **IPMI** 암호를 변경합니다

노드에 대한 원격 IPMI 액세스 권한이 있는 즉시 기본 IPMI(Intelligent Platform Management Interface) 관리자 암호를 변경할 수 있습니다. 설치 업데이트가 있는 경우 이 작업을 수행할 수 있습니다.

노드에 대한 IPM 액세스 구성에 대한 자세한 내용은 을 "각 노드에 대해 IPMI를 구성합니다"참조하십시오.

다음 노드의 IPM 암호를 변경할 수 있습니다.

- H410S 노드
- H610S 노드

H410S 노드의 기본 **IPMI** 암호를 변경합니다

IPMI 네트워크 포트를 구성하는 즉시 각 스토리지 노드에서 IPMI 관리자 계정의 기본 암호를 변경해야 합니다.

필요한 것

각 스토리지 노드에 대해 IPMI IP 주소를 구성해야 합니다.

단계

1. IPMI 네트워크에 연결할 수 있는 컴퓨터에서 웹 브라우저를 열고 해당 노드의 IPMI IP 주소를 찾습니다.
2. 로그인 프롬프트에 사용자 이름과 `ADMIN` 암호를 `ADMIN` 입력합니다.
3. 로그인 시 * 구성 * 탭을 클릭합니다.
4. 사용자 * 를 클릭합니다.
5. `ADMIN`사용자를 선택하고 * 사용자 수정 * 을 클릭합니다.
6. 암호 변경 * 확인란을 선택합니다.
7. 암호 * 및 * 암호 확인 * 필드에 새 암호를 입력합니다.
8. 수정 * 을 클릭한 다음 * 확인 * 을 클릭합니다.
9. 기본 IPMI 암호가 있는 다른 H410S 노드에 대해 이 절차를 반복합니다.

H610S 노드의 기본 **IPMI** 암호를 변경합니다

IPMI 네트워크 포트를 구성하는 즉시 각 스토리지 노드에서 IPMI 관리자 계정의 기본 암호를 변경해야 합니다.

필요한 것

각 스토리지 노드에 대해 IPMI IP 주소를 구성해야 합니다.

단계

1. IPMI 네트워크에 연결할 수 있는 컴퓨터에서 웹 브라우저를 열고 해당 노드의 IPMI IP 주소를 찾습니다.
2. 로그인 프롬프트에 사용자 이름과 `root` 암호를 `calvin` 입력합니다.
3. 로그인하면 페이지 왼쪽 상단의 메뉴 탐색 아이콘을 클릭하여 측면 표시줄 서랍을 엽니다.
4. 설정 * 을 클릭합니다.

5. 사용자 관리 * 를 클릭합니다.
6. 목록에서 * Administrator * 사용자를 선택합니다.
7. 암호 변경 * 확인란을 활성화합니다.
8. 암호 * 및 * 암호 확인 * 필드에 강력한 새 암호를 입력합니다.
9. 페이지 하단의 * 저장 * 을 클릭합니다.
10. 기본 IPMI 암호가 있는 다른 H610S 노드에 대해 이 절차를 반복합니다.

자세한 내용을 확인하십시오

- "SolidFire 및 Element 소프트웨어 설명서"
- "vCenter Server용 NetApp Element 플러그인"