



BMC 인터페이스 구성

StorageGRID 11.5

NetApp
April 11, 2024

목차

BMC 인터페이스 구성	1
BMC 인터페이스의 루트 암호 변경	1
BMC 관리 포트의 IP 주소 설정	2
BMC 인터페이스 액세스	4
서비스 어플라이언스에 대한 SNMP 설정을 구성합니다	6
알림에 대한 이메일 알림을 설정합니다	6

BMC 인터페이스 구성

서비스 어플라이언스의 BMC(베이스보드 관리 컨트롤러)에 대한 사용자 인터페이스는 하드웨어에 대한 상태 정보를 제공하고 서비스 어플라이언스에 대한 SNMP 설정 및 기타 옵션을 구성할 수 있도록 합니다.

단계

- "BMC 인터페이스의 루트 암호 변경"
- "BMC 관리 포트의 IP 주소 설정"
- "BMC 인터페이스 액세스"
- "서비스 어플라이언스에 대한 SNMP 설정을 구성합니다"
- "알림에 대한 이메일 알림을 설정합니다"

BMC 인터페이스의 루트 암호 변경

보안을 위해 BMC 루트 사용자의 암호를 변경해야 합니다.

필요한 것

관리 클라이언트가 지원되는 웹 브라우저를 사용하고 있습니다.

이 작업에 대해

어플라이언스를 처음 설치할 때 BMC는 루트 사용자에게 대한 기본 암호를 사용합니다 (root/calvin)를 클릭합니다. 시스템을 보호하려면 루트 사용자의 암호를 변경해야 합니다.

단계

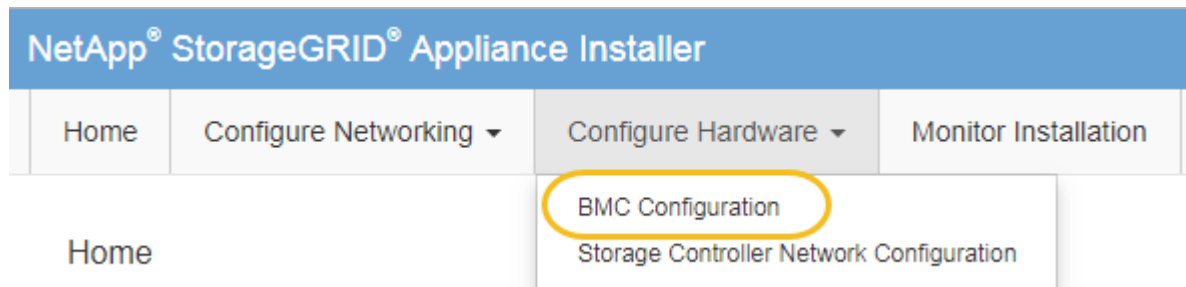
1. 클라이언트에서 StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다

https://services_appliance_IP:8443

용 services_appliance_IP, StorageGRID 네트워크에서 어플라이언스의 IP 주소를 사용합니다.

StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.

2. 하드웨어 구성 * > * BMC 구성 * 을 선택합니다.



베이스보드 관리 컨트롤러 구성 페이지가 나타납니다.

3. 제공된 두 필드에 루트 계정에 대한 새 암호를 입력합니다.

Baseboard Management Controller Configuration

User Settings

Root Password

.....

Confirm Root Password

.....

4. 저장 * 을 클릭합니다.

BMC 관리 포트의 IP 주소 설정

BMC 인터페이스에 액세스하려면 먼저 서비스 어플라이언스에서 BMC 관리 포트의 IP 주소를 구성해야 합니다.

필요한 것

- 관리 클라이언트가 지원되는 웹 브라우저를 사용하고 있습니다.
- StorageGRID 네트워크에 연결할 수 있는 관리 클라이언트를 사용 중입니다.
- BMC 관리 포트가 사용하려는 관리 네트워크에 연결되어 있습니다.
- SG100 BMC 관리 포트 *



- SG1000 BMC 관리 포트 *



이 작업에 대해



지원을 위해 BMC 관리 포트를 사용하면 낮은 수준의 하드웨어 액세스가 가능합니다. 이 포트는 안전하고 신뢰할 수 있는 내부 관리 네트워크에만 연결해야 합니다. 이러한 네트워크를 사용할 수 없는 경우 기술 지원 부서에서 BMC 연결을 요청하지 않는 한 BMC 포트는 연결되지 않거나 차단된 상태로 둡니다.

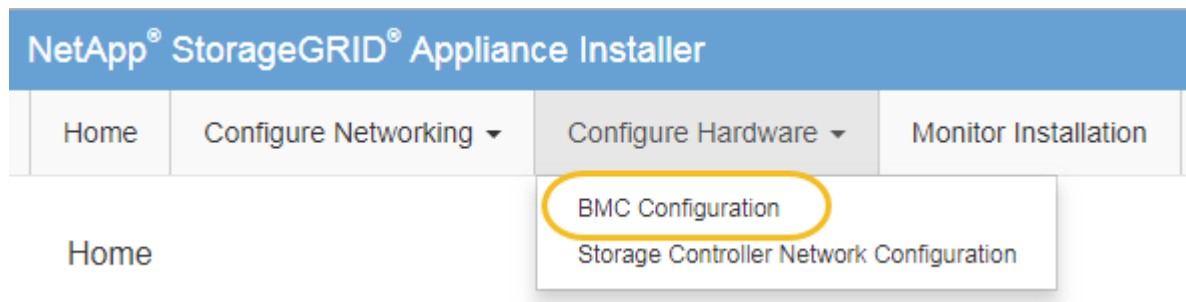
단계

1. 클라이언트에서 StorageGRID 어플라이언스 설치 프로그램의 URL을 입력합니다
`https://services_appliance_IP:8443`

용 `services_appliance_IP`, StorageGRID 네트워크에서 어플라이언스의 IP 주소를 사용합니다.

StorageGRID 어플라이언스 설치 관리자 홈 페이지가 나타납니다.


2. 하드웨어 구성 * > * BMC 구성 * 을 선택합니다.



베이스보드 관리 컨트롤러 구성 페이지가 나타납니다.

3. 자동으로 표시되는 IPv4 주소를 기록해 둡니다.

DHCP는 이 포트에 IP 주소를 할당하는 기본 방법입니다.


 DHCP 값이 나타나려면 몇 분 정도 걸릴 수 있습니다.

Baseboard Management Controller Configuration

LAN IP Settings

IP Assignment	<input type="radio"/> Static <input checked="" type="radio"/> DHCP
MAC Address	<input type="text" value="d8:c4:97:28:50:62"/>
IPv4 Address (CIDR)	<input type="text" value="10.224.3.225/21"/>
Default gateway	<input type="text" value="10.224.0.1"/>

4. 필요에 따라 BMC 관리 포트에 대한 정적 IP 주소를 설정합니다.

 BMC 관리 포트에 고정 IP를 할당하거나 DHCP 서버의 주소에 영구 임대를 할당해야 합니다.

- Static * 을 선택합니다.
- CIDR 표기법을 사용하여 IPv4 주소를 입력합니다.
- 기본 게이트웨이를 입력합니다.

LAN IP Settings

IP Assignment	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
MAC Address	d8:c4:97:28:50:62
IPv4 Address (CIDR)	10.224.3.225/21
Default gateway	10.224.0.1

d. 저장 * 을 클릭합니다.

변경 사항을 적용하는 데 몇 분 정도 걸릴 수 있습니다.

BMC 인터페이스 액세스

BMC 관리 포트의 DHCP 또는 고정 IP 주소를 사용하여 서비스 어플라이언스에서 BMC 인터페이스에 액세스할 수 있습니다.

필요한 것

- 관리 클라이언트가 지원되는 웹 브라우저를 사용하고 있습니다.
- 서비스 어플라이언스의 BMC 관리 포트는 사용하려는 관리 네트워크에 연결되어 있습니다.
- SG100 BMC 관리 포트 *



- SG1000 BMC 관리 포트 *



단계

1. BMC 인터페이스의 URL을 입력합니다 **https://BMC_Port_IP**

용 *BMC_Port_IP*, BMC 관리 포트에 대해 DHCP 또는 고정 IP 주소를 사용합니다.

BMC 로그인 페이지가 나타납니다.

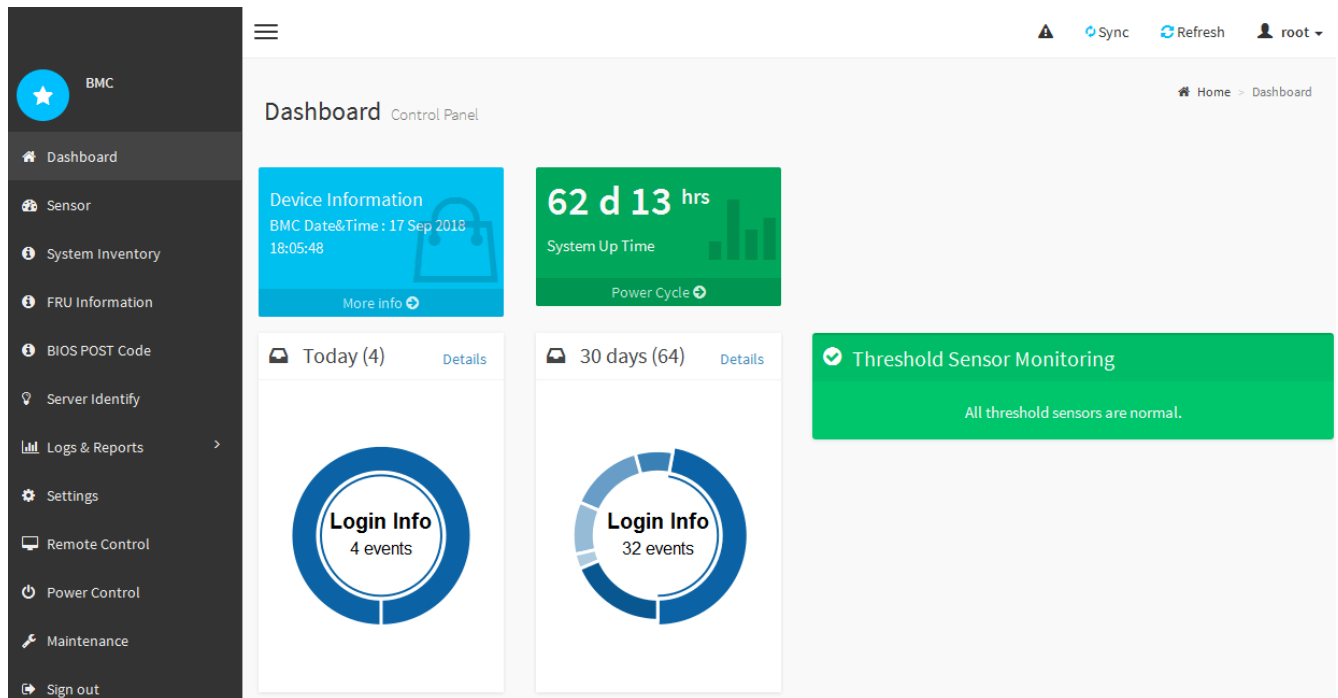
2. 기본 루트 암호를 변경할 때 설정한 암호를 사용하여 루트 사용자 이름과 암호를 입력합니다 **root**

password

A login form with a light gray background. It contains a username input field with 'root' entered, a password input field with masked characters, a 'Remember Username' checkbox, a blue 'Sign me in' button, and a link 'I forgot my password' below the button.

3. 로그인 * 을 클릭합니다

BMC 대시보드가 나타납니다.



4. 선택적으로 * 설정 * > * 사용자 관리 * 를 선택하고 "사용 안 함" 사용자를 클릭하여 추가 사용자를 생성합니다.



사용자가 처음 로그인할 때 보안을 강화하기 위해 암호를 변경하라는 메시지가 표시될 수 있습니다.

관련 정보

서비스 어플라이언스에 대한 SNMP 설정을 구성합니다

하드웨어에 대한 SNMP 구성에 익숙한 경우 BMC 인터페이스를 사용하여 서비스 어플라이언스에 대한 SNMP 설정을 구성할 수 있습니다. 보안 커뮤니티 문자열을 제공하고, SNMP 트랩을 활성화하고, 최대 5개의 SNMP 대상을 지정할 수 있습니다.

필요한 것

- BMC 대시보드에 액세스하는 방법을 알고 있습니다.
- SNMPv1-v2c 장비에 대한 SNMP 설정을 구성한 경험이 있습니다.

단계

1. BMC 대시보드에서 * 설정 * > * SNMP 설정 * 을 선택합니다.
2. SNMP 설정 페이지에서 * SNMP V1/V2 * 활성화 를 선택한 다음 읽기 전용 커뮤니티 문자열과 읽기/쓰기 커뮤니티 문자열을 제공합니다.

읽기 전용 커뮤니티 문자열은 사용자 ID 또는 암호와 같습니다. 침입자가 네트워크 설정에 대한 정보를 얻지 못하게 하려면 이 값을 변경해야 합니다. 읽기-쓰기 커뮤니티 문자열은 인증되지 않은 변경으로부터 장치를 보호합니다.

3. 필요에 따라 * 트랩 사용 * 을 선택하고 필요한 정보를 입력합니다.



IP 주소를 사용하여 각 SNMP 트랩의 대상 IP를 입력합니다. 정규화된 도메인 이름은 지원되지 않습니다.

서비스 어플라이언스가 비정상 상태일 때 SNMP 콘솔에 즉시 알림을 보내도록 하려면 트랩을 활성화합니다. 트랩은 링크 상승/하강 상태, 특정 임계값을 초과하는 온도 또는 높은 트래픽을 나타낼 수 있습니다.

4. 필요에 따라 * 테스트 트랩 전송 * 을 클릭하여 설정을 테스트합니다.
5. 설정이 올바르면 * 저장 * 을 클릭합니다.

알림에 대한 이메일 알림을 설정합니다

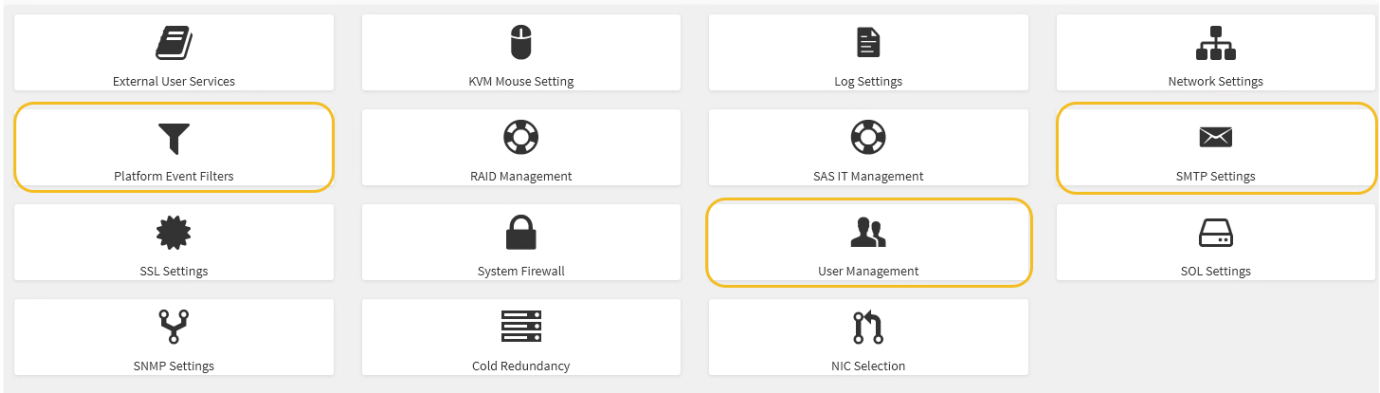
경고가 발생할 때 e-메일 알림을 보내려면 BMC 인터페이스를 사용하여 SMTP 설정, 사용자, LAN 대상, 경고 정책 및 이벤트 필터를 구성해야 합니다.

필요한 것

BMC 대시보드에 액세스하는 방법을 알고 있습니다.

이 작업에 대해

BMC 인터페이스에서 설정 페이지의 * SMTP 설정 * , * 사용자 관리 * 및 * 플랫폼 이벤트 필터 * 옵션을 사용하여 이메일 알림을 구성합니다.



단계

1. SMTP 설정을 구성합니다.

- a. 설정 * > * SMTP 설정 * 을 선택합니다.
- b. 보낸 사람 e-메일 ID의 경우 유효한 e-메일 주소를 입력합니다.

이 전자 메일 주소는 BMC가 전자 메일을 보낼 때 보내는 사람 주소로 제공됩니다.

2. 알림을 받도록 사용자를 설정합니다.

- a. BMC 대시보드에서 * 설정 * > * 사용자 관리 * 를 선택합니다.
- b. 알림 알림을 수신할 사용자를 한 명 이상 추가하십시오.

사용자에 대해 구성한 전자 메일 주소는 BMC가 경고 알림을 보내는 주소입니다. 예를 들어 "notification-user"와 같은 일반 사용자를 추가하고 기술 지원 팀 이메일 배포 목록의 이메일 주소를 사용할 수 있습니다.

3. 경고를 위한 LAN 대상을 구성합니다.

- a. 설정 * > * 플랫폼 이벤트 필터 * > * LAN 대상 * 을 선택합니다.
- b. LAN 대상을 하나 이상 구성합니다.
 - 대상 유형으로 * 이메일 * 을 선택합니다.
 - BMC Username 에서 이전에 추가한 사용자 이름을 선택합니다.
 - 여러 사용자를 추가했으며 모든 사용자가 알림 이메일을 받도록 하려면 각 사용자에 대해 LAN 대상을 추가해야 합니다.
- c. 테스트 알림을 보냅니다.

4. BMC가 경고를 보내는 시기와 위치를 정의할 수 있도록 경고 정책을 구성합니다.

- a. 설정 * > * 플랫폼 이벤트 필터 * > * 경고 정책 * 을 선택합니다.
- b. 각 LAN 대상에 대해 하나 이상의 경고 정책을 구성합니다.
 - 정책 그룹 번호 로 * 1 * 을 선택합니다.
 - 정책 작업의 경우 * 항상 이 대상으로 알림 전송 * 을 선택합니다.
 - LAN 채널의 경우 * 1 * 을 선택합니다.
 - 대상 선택기에서 정책의 LAN 대상을 선택합니다.

5. 다양한 이벤트 유형에 대한 경고를 적절한 사용자에게 보내도록 이벤트 필터를 구성합니다.
 - a. 설정 * > * 플랫폼 이벤트 필터 * > * 이벤트 필터 * 를 선택합니다.
 - b. 경고 정책 그룹 번호 에 * 1 * 을 입력합니다.
 - c. 경고 정책 그룹에 알림을 보낼 모든 이벤트에 대한 필터를 만듭니다.
 - 전원 동작, 특정 센서 이벤트 또는 모든 이벤트에 대한 이벤트 필터를 만들 수 있습니다.
 - 모니터링할 이벤트를 잘 모르는 경우 센서 유형에 대해 * All Sensors * 를 선택하고 이벤트 옵션에 대해 * All Events * 를 선택합니다. 원치 않는 알림을 받으면 나중에 선택 사항을 변경할 수 있습니다.

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.