NETAŞ Sunucu

BMC Kullanıcı Kılavuzu (BMC V4)

Sürüm: R1.0

Yenişehir Mahallesi, Osmanlı Bulvarı, Esas Aeoropark Binası, Dış Kapı No: 11 B, İç Kapı No: 40 / Pendik / İstanbul

Posta Kodu : 34912

Tel: +90 (216) 522 20 00

URL: www.netas.com.tr

E-mail: info@netas.com.tr

Revizyon Geçmişi

Revizyon No.	Revizyon Tarihi	Revizyon Sebebi
R1.0	01 Ekim 2023	Birinci baskı.

Yayımlanma Tarihi: 2023-10-01 (R1.0)

İçindekiler Tablosu

Bu El Kitabı Hakkında

Amaç

Bu kılavuzda, BMC'nin konfigürasyonu ve yönetimi ile ilgili olarak yol göstermek üzere NETAŞ sunucularının BMC yönetim yazılımı açıklanmıştır.

Hedeflenen Okuyucu Kitlesi

Bu el kitabı hazırlanırken aşağıdaki kitle hedeflenmiştir:

- Ağ planlama mühendisleri
- Konfigürasyon mühendisleri
- Bakım mühendisleri

Bu El Kitabında Neler Var?

Bu El Kitabı aşağıdaki bölümlerden oluşmaktadır:

Bölüm 1, BMC'ye Genel Bakış	BMC'nin çalışma prensibi ve işlevlerini, yazılım güvenliği ve işletim arayüzlerini açıklar.
Bölüm 2, İstemcinin Devreye Alınması	Bir İstemci aracılığıyla oturum açılan BMC Web portalında gerçekleştirilen hata ayıklama işlemlerini açıklar.
Bölüm 3, BMC'nin Web Portalında Oturum Açma	BMC'nin Web portalında nasıl oturum açılabileceğini açıklar.
Bölüm 4, Genel İşlemler	BMC'de gerçekleştirilen genel işlemleri açıklar.
Bölüm 5, Sistem Yönetimi	Sistem yönetimi işlemlerinin nasıl gerçekleştirildiğini açıklar.
Bölüm 6, Arıza Tespiti ve Bakım	Arıza tespiti ve bakım işlemlerinin nasıl gerçekleştirildiğini açıklar.
Bölüm 7, Hizmet Yönetimi	Hizmet yönetimi işlemlerinin nasıl gerçekleştirildiğini açıklar.
Bölüm 8, BMC Yönetimi	BMC yönetimi işlemlerinin nasıl gerçekleştirildiğini açıklar.
Bölüm 9, Kullanıcı ve Güvenlik	Kullanıcı ve güvenlik yönetimi işlemlerinin nasıl gerçekleştirildiğini açıklar.

Bölüm 10, Referans: Dokümanlara Erişim	Dokümanlara erişim adımlarını açıklar

Kurallar / Gösterim Biçimleri

Bu El Kitabı aşağıdaki gösterim biçimlerinden faydalanmaktadır.

	İkaz: Ekipman veya ortam güvenliği bilgilerini belirtir. Kurallara uyulmaması ekipmanda hasara, veri kaybına, ekipman performansında düşüşe, çevresel kirlenmeye ve diğer tahmin edilemeyen sonuçlara yol açabilir.
	Not: Bir konu hakkında ilave bilgiler sağlar.

Bölüm 1
BMC Genel Açıklaması

İçindekiler Tablosu

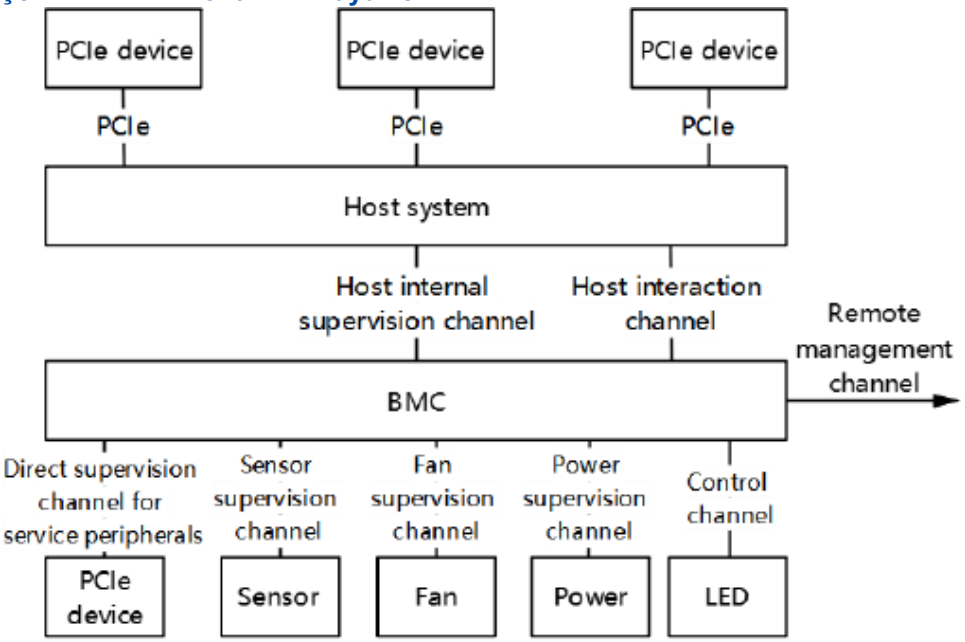
BMC, sunucu donanımını izleyen ve yöneten bir NETAŞ sunucusu yönetim sistemi olup işletim ve bakım için bir Web portalı sağlar, yazılım ve donanım konfigürasyonu, arıza tespiti, işletim sistemi kurulumu ve sunucu üzerinde gerçekleştirilen işlemler için arşivleme yapar.

1.1 Çalışma Prensibi

BMC, özel bir yönetim çipi ve bu çip üzerinde çalışan bir yönetim yazılımından oluşur.

- Özel yönetim çipi
  Sunucuya özel yönetim çipi, birçok donanım arayüzü ve işlevi sağlar. BMC'nin donanım arayüzleri için Şekil 1-1'e bakınız.

Şekil 1-1 BMC Donanım Arayüzleri



BMC kanallarının açıklaması için, Tablo 1-1'e bakınız.

Tablo 1-1 BMC Donanım Kanalı Açıklamaları

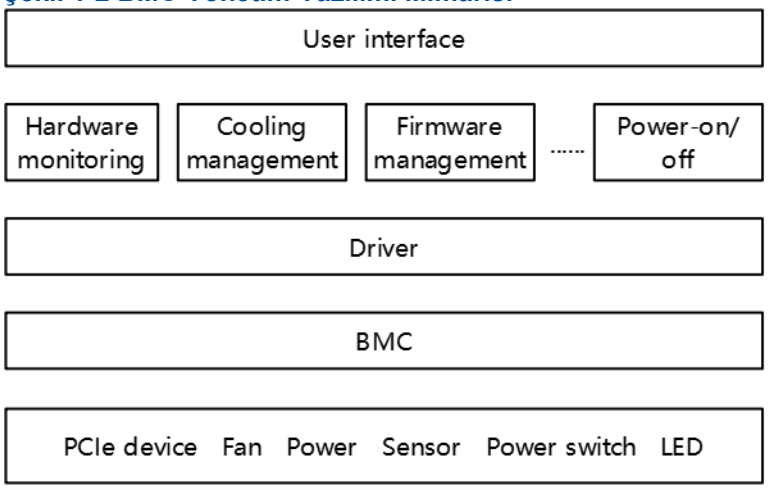
Kanal	Tipik Fiziksel Link	Tipik Yönetim Nesnesi veya İşlevi
Servis çevre birimi denetim kanalı	PCIe ve SMBUS	Bir sunucunun PCIe cihazları
Host dahili denetim kanalı	SMBUS ve PECI	CPU veya köprü çipinin dahili işlevsel birimleri
Host etkileşim kanalı	PCIe, USB, LPC, KCS ve SM-BUS	KVM'yi, sanal ortam işlevini ve host seri port işlevlerini ve IP-MI protokolünü destekler.
Hizmet çevre birimleri için doğrudan denetim kanalı	SMBUS ve NC-SI	Bir sunucunun PCIe cihazları
Sensör denetim kanalı	SMBUS, GPIO ve A/D	Sıcaklık sensörü, gerilim sensörü, akım sensörü ve varlık sensörü
Fan denetim kanalı	PWM	Fan
Güç denetim kanalı	SMBUS	CRPS ve PMBUS güç kaynağı

Kontrol kanalı	GPIO ve SGPIO	Açma, kapatma ve gösterge açık/kapalı
Uzaktan yönetim kanalı	Ethernet	BMC yönetim sunucusuna erişir

- Yönetim yazılımı

  BMC yönetim yazılımı, donanımı izlemek ve yönetmek için yönetim kanalları üzerinden donanım cihazları ile iletişim kurar. BMC yönetim yazılımının mimarisi için Şekil 1-2'ye bakınız.

Şekil 1-2 BMC Yönetim Yazılımı Mimarisi



1.2 İşlevler

BMC, bir sunucu yönetim sistemidir. Birçok yönetim işlevi sağlar.

- Sunucu sağlık durumu yönetimi: Bir sunucunun operasyonel durumunu kontrol eder, geçmiş verileri ve gerçek izleme verilerini analiz eder ve kullanıcıların sorunları önceden bulup çözmesine çözmesine yardımcı olur ve böylece sunucunun son derece güvenilir bir şekilde çalışmasını sağlar.
  - → 80 kodlu kayıt işlevi, başlatma hatalarını analiz etmek için yeterli bilgi sağlar.
  - → Sistem çöktüğünde, son ekran yakalama işlevi, sistem çökmelerini analiz etmek amacıyla sahadaki senaryoyu kaydeder.
  - → Önleyici bakım ve işletim süreçlerine ilişkin anlık ekran durum görüntüleri ve ekran kaydı, takip denetimlerini kolaylaştırır.
  - → Alarm işlevi bileşen bazlı hassas arıza tespitini destekler ve bileşen arızalarının yerinin tespit edilmesini ve arızalı bileşenin değiştirilmesini kolaylaştırır.
  - → CrashDump işlevi sistem hatalarının daha ayrıntılı analiz edilmesini kolaylaştırır.

→ BMC, alarmları raporlamak ve böylece NMS'nin sunucu arıza bilgilerini kolaylıkla toplayabilmesini sağlamak için syslog, SNMP trap, e-posta ve Redfish aboneliği işlevlerini destekler.

→ BMC, alarm göstergesi aracılığıyla sunucunun sağlık durumunun (health status) doğrudan görüntülenmesini destekler.

- Host sistem bakımı
  → Host sistemin uzaktan bakımı için sanal KVM ve sanal ortam işlevlerini destekler.
  → RAID'lerin bant-dışı izlenme ve yönetimini destekler, bu sayede RAID'ler host sisteme bağlı olunmaksızın izlenebilir ve host sistemdeki depolama cihazları yapılandırılabilir, bu da yapılandırma verimliliğini ve yönetim yeteneğini geliştirir.
  → PXE aracılığıyla OS (İşletim Sistemi) kurulumunu destekler, bu da işletim sistemlerinin toplu olarak uzaktan kurulum verimliliğini arttırır.

- Cihaz firmware (donanım yazılımı) yönetimi
  → Güvenilir işletimi sağlamak üzere çift BMC'ler desteklenir.
  → BIOS yükseltme ve işletiminin güvenilirliğini artırmak için çift BIOS desteklenir.
  → Firmware (örneğin, FRU ve EPLD) yükseltme işlevi desteklenir.

- Sistem soğutma
  → Önemli sunucu bileşenlerinin sıcaklığını izler ve farklı donanım termal özelliklerine göre farklı soğutma kontrollerini gerçekleştirir.
  → Sunucu donanımının hasar görmemesini sağlamak amacıyla aşırı sıcaklık durumunda kapatma işlevini destekler, bu da bileşenlerin hizmet ömrünü uzatır.

- Akıllı güç tüketimi yönetimi
  → BMC, power capping teknolojisini destekler ve NMS tarafından merkezi kontrol için standart DCMI sağlayarak sunucuların dağıtım/konuşlandırma yoğunluğunu artırır.
  → Enerji tasarrufu sağlayan tasarımı, sunucu işletme maliyetlerini azaltır.

- BMC öz yönetimi
  → BMC zamanını ağ ve host üzerinden senkronize ederek farklı senaryolardaki gereksinimleri karşılamayı destekler.
  → Çoklu kimlik doğrulama modlarını destekleyerek sunucu yönetimini kolaylaştırır.
  → DHCP ve DNS'yi destekleyerek sunucu dağıtımını/konuşlandırmasını ve yönetimini kolaylaştırır.

- Çeşitlendirilmiş yönetim arayüzleri

  BMC aşağıdakileri sağlayarak, çeşitli sistem entegrasyonu arayüzlerinin gereksinimlerini karşılar.

  → Standart DCMI1.5/IPMI2.0/Redfish arayüzleri
  → Uzaktan komut satırı arayüzleri ve Web yönetimi arayüzleri
  → SNMPv2 ve SNMPv3 arayüzleri

1.3 Yazılım Güvenliği

İşlev Çağırma için Güvenlik Önlemleri

- Eksiksiz güvenlik tasarımı: Güvenlik tasarımı için tehdit modellemesini (threat modeling) kullanır.
- Şifrelenmiş KVM erişimi: Şifrelenmiş KVM erişimini destekler.
- Yüksek şifreleme güvenlik seviyesine sahip HTTPS erişimi: Web sayfası üzerinden sisteme oturum açtıklarında lokal veya uzak kullanıcıları korumak ve iletişim verilerinin değiştirilmesini veya sızdırılmasını önlemek amacıyla sunucu ve kullanıcılar arasında bir HTTPS güvenilir yolu (trusted path) sağlar.
- Yüksek şifreleme güvenlik seviyesine sahip SSH erişimi: Sisteme oturum açtıklarında lokal veya uzak kullanıcıları korumak ve iletişim verilerinin değiştirilmesini veya sızdırılmasını önlemek amacıyla sunucu ile kullanıcılar arasında ve sunucular ve diğer cihazlar arasında bir SSH güvenilir yolu (trusted path) sağlar.
- Yüksek şifreleme güvenlik seviyesine sahip SNMPv3 protokolü: SNMPv3 iletişim güvenlik protokolü, SHA ve AES'yi destekler.
- Yüksek şifreleme güvenlik seviyesine sahip IPMI 2.0 protokolü: IPMI 2.0 iletişim protokolünü destekler ve daha yüksek seviyeli bir şifreleme güvenlik teknolojisi sağlar.
- Yüksek şifreleme güvenlik seviyesine sahip Redfish arayüzü: IPMI protokolünden daha yüksek seviyeli bir şifreleme ile yeni nesil standart raf yönetim arayüzünü destekler.
- Protokol ve port saldırısına karşı koruma: Kullanılmayan ağ hizmetlerini ve yüksek riskli portları ve aynı zamanda varsayılan olarak RMCP, Telnet ve HTTP dahil olmak üzere güvenli olmayan protokolleri devre dışı bırakır.

Kullanıcı İzinleri için Güvenlik Önlemleri

- Kullanıcı rol yönetimi: Kullanıcı izinleri, oturum açmış olan kullanıcılara tahsis edilir, birden fazla yönetim kullanıcı rolü tahsis etmek mümkündür. Roller farklı seviyelere ayrılabilir. Roller ilişkilendirilerek, yetkisiz işlemleri önlemek amacıyla her bir kullanıcının işlevsel izinleri kısıtlanabilir.
- Kullanıcı hesabı güvenliğinin arttırılması: Zayıf parola algılama, varsayılan güçlü parola, parola karmaşıklığının yapılandırması, parola geçerlilik süresinin yapılandırması ve parola değişikliği esnasında en son kullanılan üç eski parolanın tekrar kullanımının yasaklanması desteklenir.
- Kimlik doğrulama hizmeti: BMC hem yerel kimlik doğrulama erişimini hem de uzaktan kimlik doğrulama erişimini destekler. Uzaktan erişim, LDAP üzerinden kimlik doğrulamayı ve oturum açma kimlik doğrulaması başarısız olduğunda hesabın kilitlenmesi özelliğini destekler. Oturum açma hatalarının sayısı yapılandırılabilir.

- Kullanıcı erişimi kısıtlama: Kullanıcı erişimi; zaman periyodu, kaynak IP adresi ve MAC whitelist'e (beyaz liste) göre kısıtlanabilir. Sistem, maksimum oturum sayısı, oturum zaman aşımı sonrasında zorunlu çıkış, yapılandırılabilir oturum sona ermesi, tek bir kullanıcı için çoklu eş zamanlı oturum kısıtlama, çevrimiçi kullanıcı yönetimi ve zorunlu oturum kapatma gibi işlevleri destekler.
- İzinsiz giriş (saldırı) alarmı: BMC, sistem güvenliğini arttırmak için şasi kapağı açılma alarmını destekler.
- Kayıp kullanıcı kimliği kimlik doğrulama bilgilerinin alınması: Eğer bir kullanıcı parolası kaybedilirse, e-posta yoluyla tekrar alınabilir.
- Sertifika hizmeti: BMC, sadece sistem yöneticisi (admin) tarafından gerçekleştirilebilecek sertifika şifreleme ve içeri aktarma hizmetlerini destekler. Sistem, güvenli sertifika imza algoritmasını destekler, sertifika geçerlilik süresinin yapılandırılmasını destekler ve sertifikanın geçerlilik süresi dolduğunda veya dolmak üzere olduğunda bildirimde bulunur.

Log Yönetimi için Güvenlik Önlemleri

- Log kaydetme: Tarih, saat, kullanıcı, olay açıklaması, olay sonucu ve diğer ilgili bilgiler dahil olmak üzere tüm ana sistem olayları kaydedilebilir. BMC, bileşen değiştirme loglarının kaydedilmesini destekler.
- Log kategorisi: BMC, işlem logları, bakım logları ve güvenlik logları dahil farklı log kategorilerini destekler.
- Log sorgulama: BMC, yetkili kullanıcılara log bilgilerini sorgulama izinlerini sağlar ve log dosyalarına yasa dışı erişilmesini önlemek amacıyla log dosyası okuma izinlerinin hesaba göre tahsis edilmesini destekler.
- Log koruma: Loglar kalıcı depolama ortamına kaydedilir. Saklanan log bilgilerinin değiştirilmesinin önlenmesi amacıyla saklanan log bilgileri izinsiz silinemez. Loglar 90 gün veya daha uzun süreyle saklanır.
- Log yedekleme: Yerel depolama alanının yetersiz olması durumunda, loglar FTP üzerinden başka depolama alanlarına aktarılabilir.
- Merkezi alarm yönetimi: BMC, cihaz çalışırken meydana gelen arızalar için merkezi alarm yönetimini destekler, yetkili kullanıcıların alarmları dışarı aktarmasına izin verir ve SNMP Trap (SNMP Tuzağı) aracılığıyla alarm raporlamasını merkezi bir şekilde destekler.
- Merkezi log yönetimi: BMC, yetkili kullanıcıların logları dışarı aktarmasına izin verir ve logları Syslog üzerinden merkezi bir şekilde destekler.
- Güvenilir zaman damgası (timestamp): BMC, sistem loglarının ve alarmların zaman referansı doğruluğunu sağlamak amacıyla yerel saat değişikliğini ve NTP'yi destekler.

Veri Güvenliği için Güvenlik Önlemleri

- Şifrelenmiş veri depolama: Veri koruma, şifrelenmiş veri depolama ve veritabanı parola kimlik doğrulamasını destekler.

- Şifrelenmiş veri iletimi: Veri iletimi güvenliğini temin etmek için KVM şifreleme işlevini ve IPMI 2.0/SNMP V3/SSH/Redfish/HTTPS gibi yüksek şifreleme güvenlik seviyelerine sahip iletişim protokollerini destekler.
- Veri bütünlüğü: Veri doğrulama, depolama ve iletimi için veri bütünlüğü kontrolünü destekler.

Sürüm Yönetimi için Güvenlik Önlemleri

- Sürüm bütünlüğü kontrolü: Sunucu sistemi yazılımı yüklediğinde BMC, iletim esnasında hata kodlarının neden olduğu sürüm karışıklığını veya kötü niyetli modifikasyonları önlemek amacıyla yazılımın bütünlüğünü kontrol eder
- Yazılım yükseltme izni kontrolü: BMC, yazılım sürümü ve firmware (donanım yazılımı) sürümü bilgilerini kaydeder. Sadece sistem yöneticisi (admin) yazılım ve firmware yükseltme ve loglardaki ilgili işlemleri kaydetme iznine sahiptir.
- Sürüm düşürme: Sürüm yükseltme işlemi esnasında bir hata meydana geldiğinde, sürüm düşürülebilir.
- Güvenlik açığı içermeyen yazılım sürümü: Ürün yazılımı yayınlanmadan önce NSFOCUS, NESSUS ve WebInspect gibi güvenlik araçları kullanılarak güvenlik taramasından geçirilir ve güvenlik açıkları için kaynak kodu aramasından geçirilir. Ek olarak, ürün yazılımı, hiçbir güvenlik açığı olmadığından emin olmak için birkaç tur sızma (penetration) testine tabi tutulur.
- Yedeklilik: BMC, aktif/standby BMC önyüklemelerini, BMC sürümlerini ve BMC yönetim portlarını destekler.
- Sıkı sürüm yayınlama kontrol süreci: BMC, kullanılan üçüncü taraf yazılımlarının ve eklentilerinin (plug-in) güvenlik değerlendirmesinin gerçekleştirilmesini destekler. BMC, bir sürüm yayınlanmadan önce bu sürümü yaygın olarak kullanılan anti-virüs yazılımları ile tarar. Onaysız sürüm değişikliklerini önlemek için SHA256 kontrol kodları yayınlanır.
- Güvenli ve kontrol edilebilir BMC kaynak kodu: BMC kaynak kodu,%100 kod walkthrough ve Klocwork ve Coverity white box güvenlik kontrollerini ve testlerini geçer, böylece potansiyel güvenlik açıkları elimine edilir ve güvenlik güçlendirilir.

1.4 İşlem Arayüzleri

BMC, genel toplu dağıtım/konuşlandırma işlem arayüzlerini ve sunucu yönetim arayüzlerini destekler.

- Toplu dağıtım/konuşlandırma işlem arayüzleri şunları içerir:
  → IPMI bir standart sunucu arayüzüdür. IPMI2.0'da belirtilen işlevleri uygulamak için host tarafındaki izleme yazılımı veya üst katman NMS ile ara bağlantı için kullanılır.

→ Redfish arayüzü bir standart sunucu arayüzüdür. Bir sunucuyu izlemek ve yönetmek için üst katman NMS ile ara bağlantı için kullanılır.

→ SNMP arayüzü standart olmayan bir sunucu arayüzüdür. Bir sunucuyu izlemek ve yönetmek için üst katman NMS ile ara bağlantı için kullanılır.

- Sunucu yönetim arayüzleri aşağıdakileri içerir:
  → Web arayüzü
  → KVM arayüzü
  → Uzak CLI

Bölüm 2
İstemci Devreye Alma İşleminin Gerçekleştirilmesi

Özet

Birçok durumda, bir istemci üzerindeki BMC'nin Web portalında, bir sunucunun iSAC yönetim ağı portu aracılığıyla oturum açabilirsiniz. BMC'nin Web portalında ilk kez oturum açmadan önce, iSAC yönetim ağı portu ile ara bağlantısının yapıldığından emin olmak için istemciyi devreye almanız gereklidir.

Önkoşul

- Aşağıda belirtilen gerekli araçların tümü hazır olmalıdır:
  - → Bir PC (istemci olarak davranan)
  - → Ağ kabloları
- Aşağıdaki tarayıcılardan biri PC üzerine halihazırda kurulu olmalıdır:
  - → Google Chrome 59 veya daha üst bir sürüm
  - → Firefox 54 veya daha üst bir sürüm
  - → Microsoft IE 11 veya daha üst bir sürüm

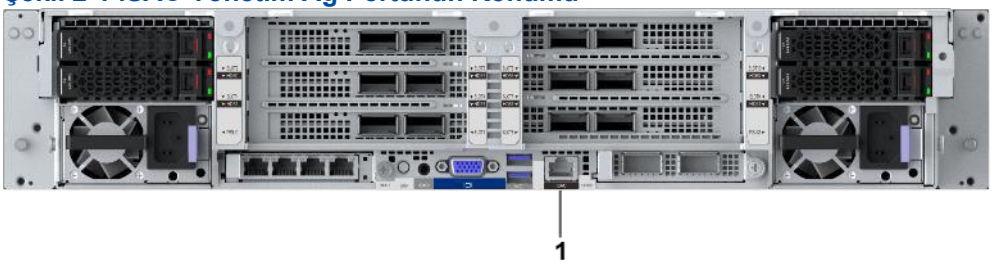
Not

Google Chrome 59 ve üzeri sürümler önerilir.

İçerik

Bir sunucunun iSAC yönetim ağ portunun varsayılan IP adresi, 192.168.5.7'dir. Şekil 2-1'de sunucunun arka panelindeki iSAC yönetim ağ portunun konumu gösterilmektedir.

Şekil 2-1 iSAC Yönetim Ağ Portunun Konumu



1. iSAC yönetim ağ portu

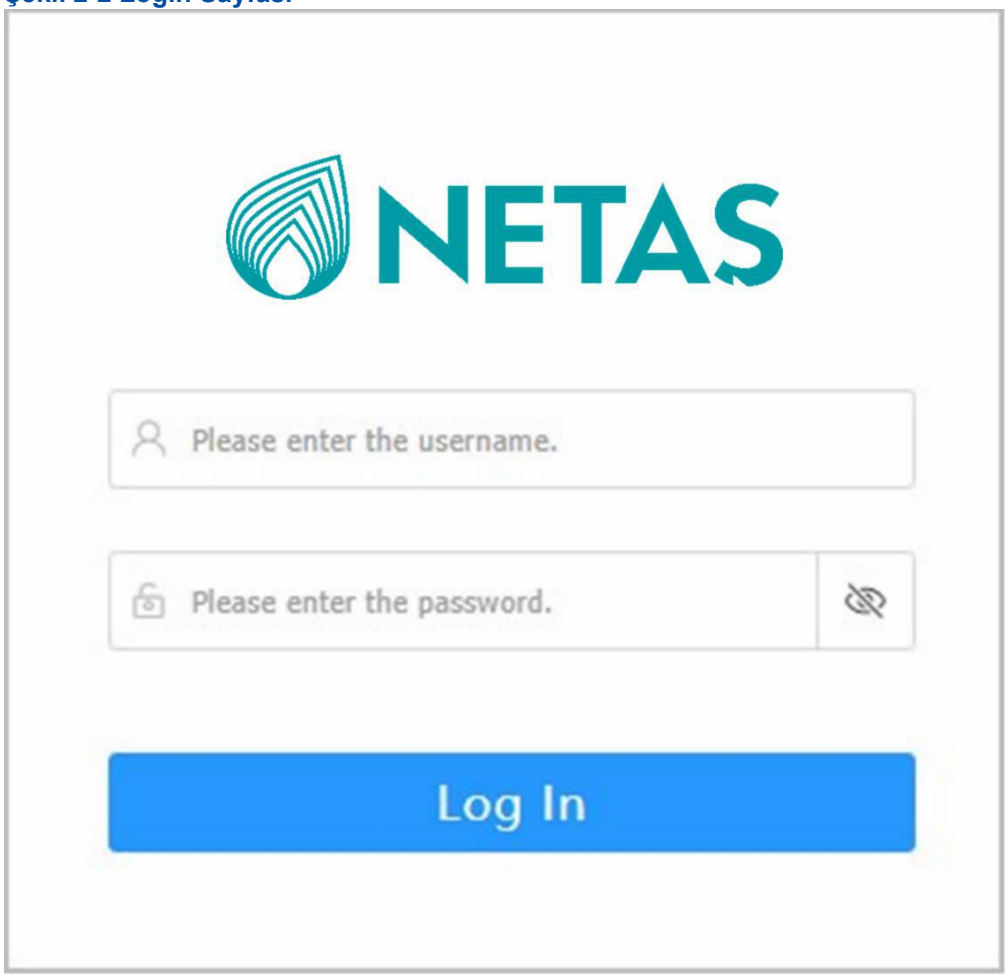
Not

Bir sunucunun arka panelindeki **iSAC** bilgi etiketli ağ portu, ıSAC yönetim ağ portunu belirtir. Bu prosedürde iSAC yönetim ağ portunun konumunu açıklamak için örnek olarak bir NCS6722 N4 sunucusu kullanılmıştır.

Adımlar

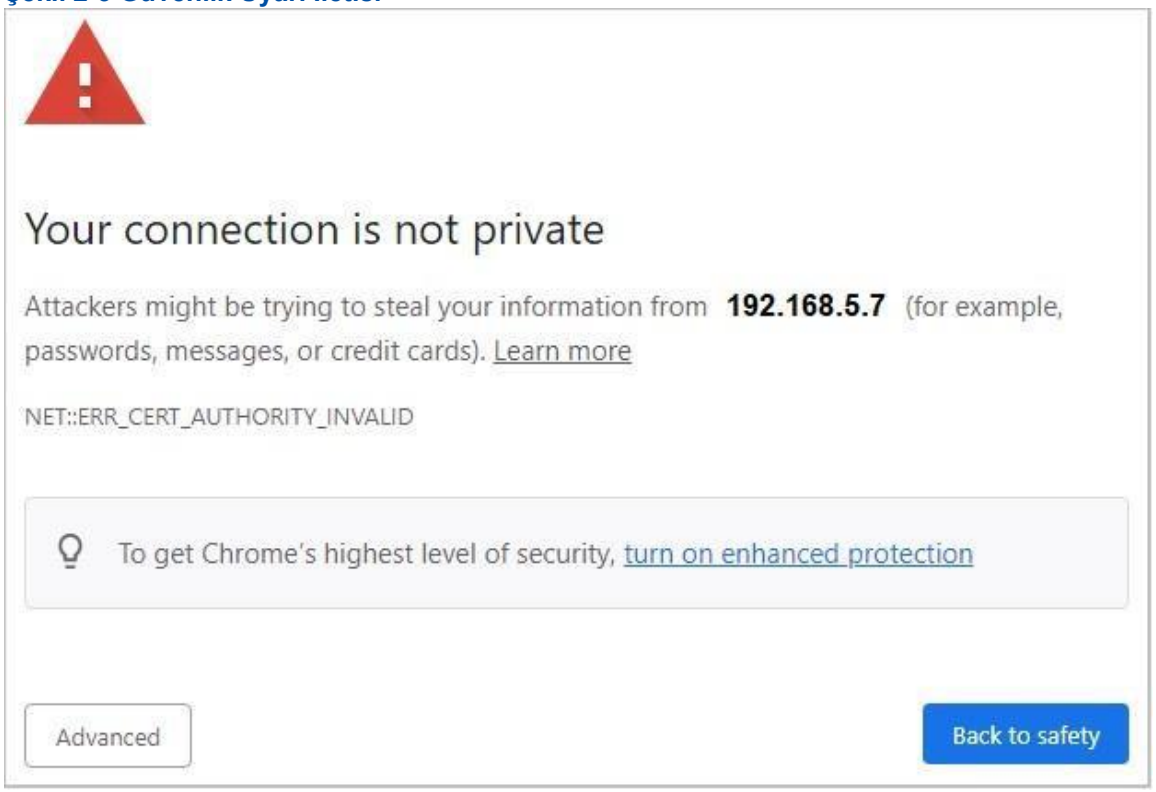
1. Bir ağ kablosu kullanarak sunucunun arka panelindeki iSAC yönetim ağ portunu PC'ye bağlayın.
2. PC üzerinde, PC'nin IP adresini 192.168.5.7 ile aynı ağ segmentindeki bir IP adresi ile değiştirin (örneğin; 192.168.5.8).
3. PC'de belirtilen tarayıcıyı başlatın.
4. Tarayıcının adres çubuğuna `https://192.168.5.7` adresini girin ve **Enter** üzerine basın. Login sayfası açılacaktır, bakınız Şekil 2-2.

Şekil 2-2 Login Sayfası



Oturum açmadan önce Şekil 2-3'te gösterilen uyarı iletisi görüntülenirse, **Advanced** üzerine tıklayın ve login sayfasına girmek için **Proceed to** seçimini yapın.

Şekil 2-3 Güvenlik Uyarı İletisi



5. Kullanıcı adınızı ve parolanızı girin.

Not

Varsayılan kullanıcı adı ve parolası aşağıdaki gibidir:

- Kullanıcı adı: root
- Parola: root12349!

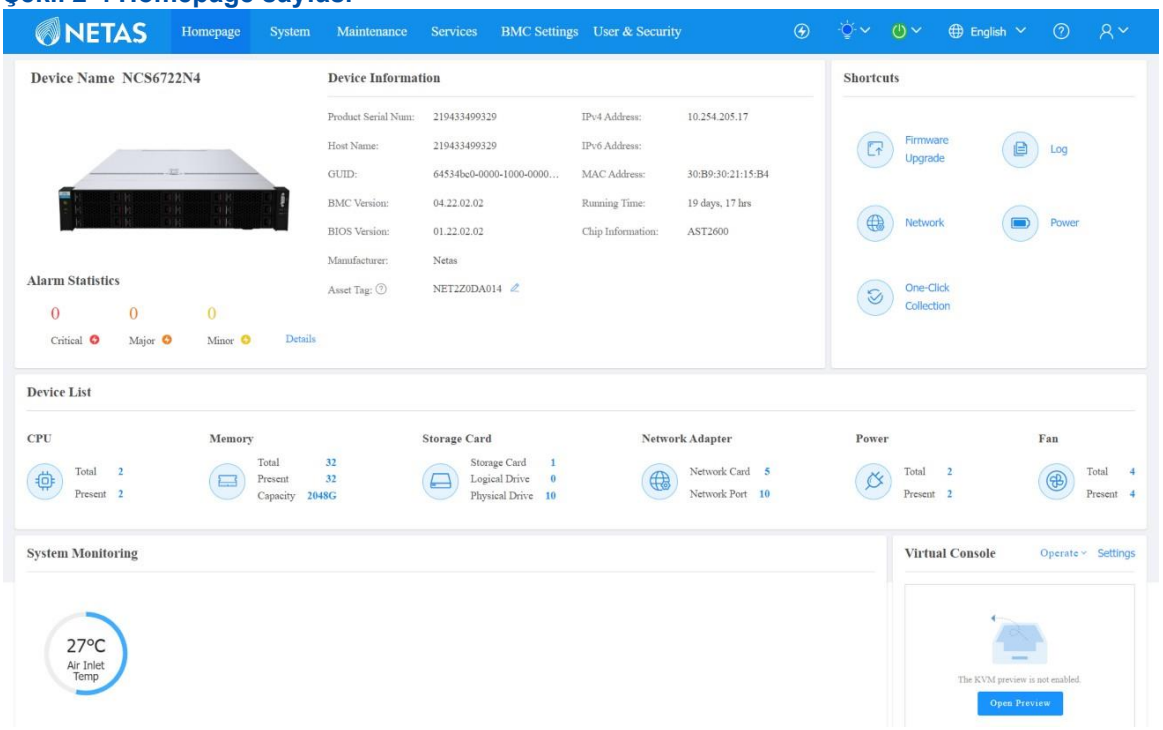
Parolayı görünür yapmak için sağdaki butonuna tıklayabilirsiniz.

Not

Varsayılan parolayı kullanarak BMC Web portalında oturum açtıktan sonra varsayılan parolayı derhal değiştirmeniz gerekir. Varsayılan parolayı güçlü bir parola ile değiştirmeniz önerilir.

6. **Log In** üzerine tıklayın. BMC Web portalının **Homepage** sayfası görüntülenir, bakınız Şekil 2-4.

Şekil 2-4 Homepage sayfası



7. iSAC yönetim ağ portunun IP adresini planlanan şekilde değiştirin, örneğin; 10.235.51.202.

Not

iSAC yönetim ağ portunun IP adresinin nasıl ayarlanacağı hakkında bilgi almak için 8.1.3 Ağ Portlarının IP Adreslerinin Yapılandırılması bölümüne başvurun.

---

8. iSAC yönetim ağ portunun IP adresini kaydedin.
9. iSAC yönetim ağ portunu bir ağ kablosu aracılığıyla ilgili anahtara bağlayın.
10. PC üzerinde, PC'nin IP adresini iSAC yönetim ağ portunun ait olduğu ağ segmentindeki bir IP adresi ile değiştirin (örneğin; 10.235.51.203).
11. PC'yi bir ağ kablosu aracılığıyla ilgili anahtara bağlayın, böylece PC ve iSAC yönetim ağ portu aynı LAN içerisinde olur.
12. PC'nin iSAC yönetim ağ portuyla düzgün bir şekilde iletişim kurabildiğinden emin olmak için PC'nin CLI'sinde **`ping`** komutunu çalıştırın.

Bölüm 3
BMC'nin Web Portalında Oturum Açma

Özet

Bu prosedürde, PC'nizdeki belirtilen tarayıcı aracılığıyla bir sunucunun BMC Web portalında nasıl oturum açılacağı açıklanmıştır. Sunucuyu portal üzerinden izleyebilir ve yönetebilirsiniz.

Önkoşul

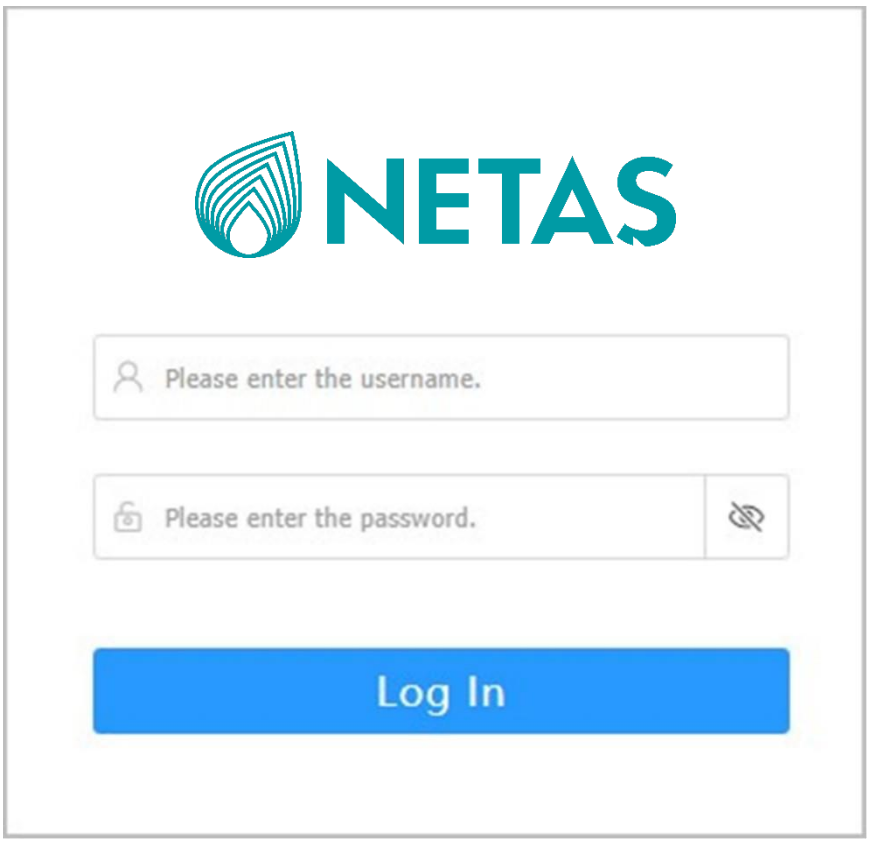
iSAC yönetim ağ portunun IP adresi halihazırda alınmış olmalıdır.

Adımlar

1. Tarayıcının adres çubuğuna BMC’nin Web portalının adresini girin ve ardından **Enter** tuşuna basın.

   . Login sayfası açılacaktır, bakınız Şekil 3-1.

Şekil 2-2 Login Sayfası

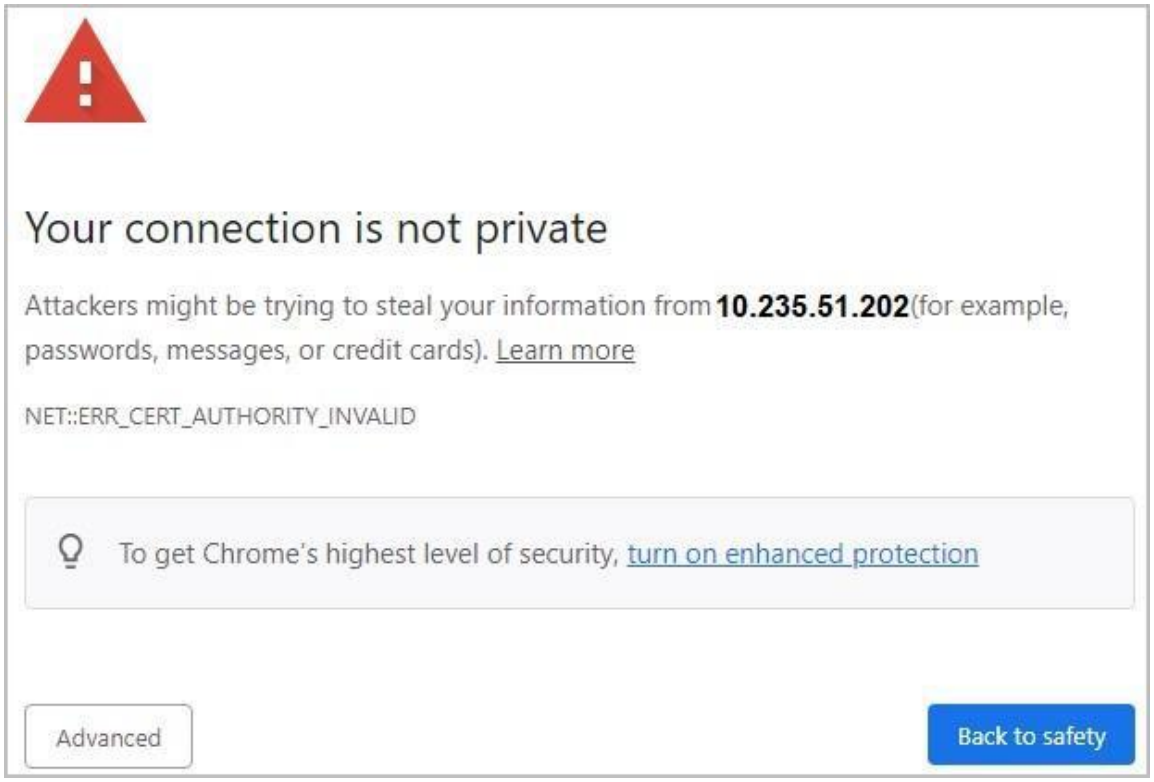


Not

BMC'nin Web portalının adresi formatı şu şekildedir: *https://IP*. "IP", iSAC yönetim ağ portunun IP adresidir.

Oturum açmadan önce Şekil 3-2'de gösterilen uyarı iletisi görüntülenirse, **Advanced** üzerine tıklayın ve login sayfasına girmek için **Proceed to** seçimini yapın.

Şekil 3-2 Güvenlik Uyarı İletisi



2. Kullanıcı adınızı ve parolanızı girin.

Not

Varsayılan kullanıcı adı ve parolası aşağıdaki gibidir:

- Kullanıcı adı: root
- Parola: root12349!

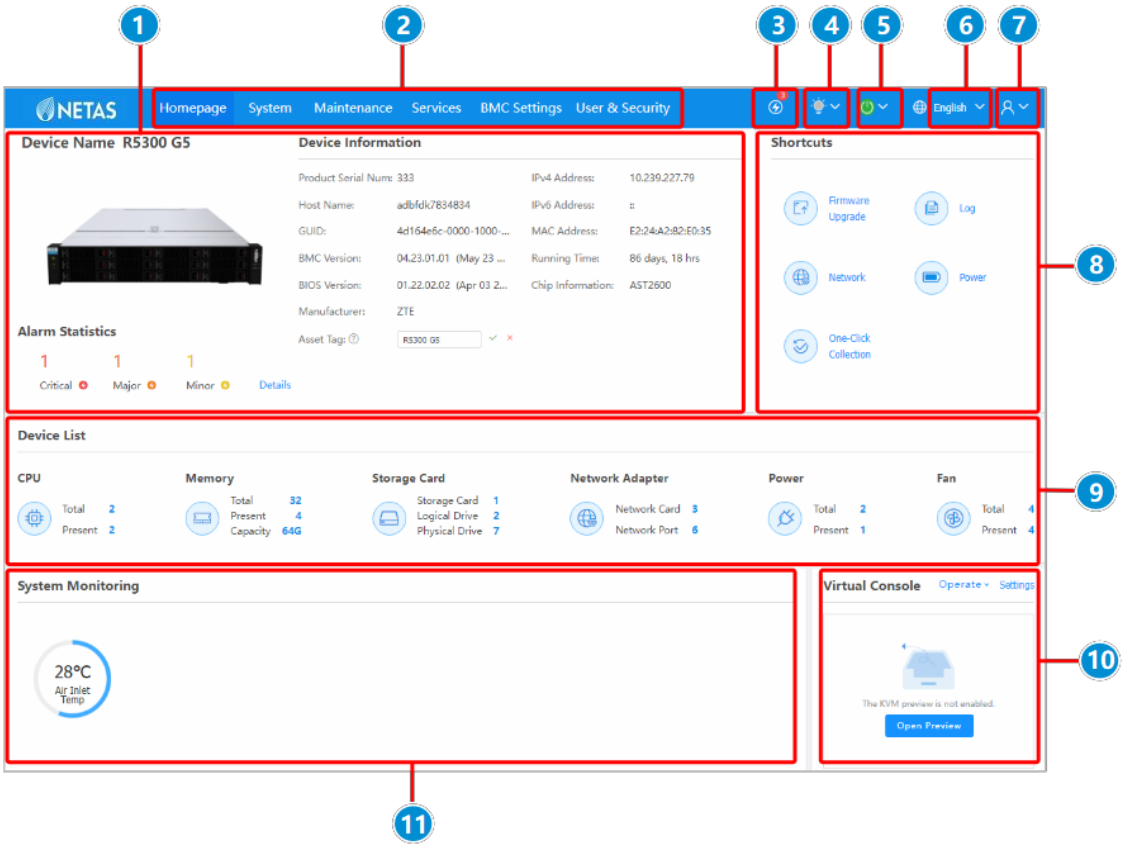
Parolayı görünür yapmak için sağdaki butonuna tıklayabilirsiniz.

Not

Varsayılan parolayı kullanarak BMC Web portalında oturum açtıktan sonra varsayılan parolayı derhal değiştirmeniz gerekir. Varsayılan parolayı güçlü bir parola ile değiştirmeniz önerilir.

3. **Log In** üzerine tıklayın. BMC Web portalının **Homepage** sayfası görüntülenir, bakınız Şekil 3-3.

Şekil 3-3 Homepage sayfası



Homepage sayfasının açıklamaları için Tablo 3-1'e başvurun.

Tablo 3-1 Homepage Sayfasının Açıklamaları

No.	Ad	Açıklama
1	**Device Information**	Sunucunun detaylı bilgilerini ve aktif alarm istatistiklerini görüntüler. • Sunucunun varlık bayrağını değiştirmek için üzerine tıklayın. • Ayrıntılarını görüntülemek için **Details** üzerine tıklayın.
2	Menü çubuğu	Menü çubuğu üzerinde herhangi bir ana menüye tıklamanızın ardından tüm işlev menülerini bir navigasyon ağacı biçiminde sol pencere içerisinde görüntüler.
3	Alarm butonu	Aktif alarmların toplam sayısını görüntüler. • Her seviyedeki alarm sayısını görmek için farenizin imlecini bu buton üzerine getirin. • Alarm ayrıntılarını görmek için bu butona tıklayın.

4	UID butonu	Sunucunun UID göstergesi durumunu görüntüler. UID göstergesinin durumunu değiştirmek için bu butona tıklayın ve ilgili kısayol menüsünü seçin. Kısayol menüsü şunları içerir: • **Sürekli yanıyor**: UID göstergesi yanar, bu sayede ekipman odasındaki sunucular arasında geçerli sunucuyu belirleyebilirsiniz.

No.	**Ad**	**Açıklama**
		• **Yanıp, sönüyor:** UID göstergesi yanıp söner, bu da BMC'nin çalıştırıldığını gösterir. BMC, Web portal, KVM veya sanal ortam kullanıldığında UID göstergesi otomatik olarak yanıp söner. • **Kapalı/Sönük:** UID göstergesi kapalı/sönüktür. Gri renkli kısayol menüsü, UID göstergesinin geçerli durumunu gösterir. Örneğin; eğer **Blink** kısayol menüsü gri renkli ise, sunucunun UID göstergesi yanıp sönmektedir.
5	Güç butonu	Sunucunun güç durumunu görüntüler. Güç durumunu değiştirmek için bu butona tıklayın ve ilgili kısayol menüsünü seçin. Kısayol menüsü şunları içerir: • **Power on:** Sunucu açılır. • **Normal Power Off**: Sunucu kapatılır.. • **Forced Power Off**: Sunucu zorla kapatılır. • **Power Reset**: Sunucu kapatılır ve daha sonra açılır. • **Power Cycle**: Güç zorla kapatılır ve daha sonra açılır. Gri renkli kısayol menüsü, sunucunun geçerli güç durumunu gösterir. Örneğin; **Power On** kısa yol menüsü gri renkli ise, sunucu güç açık durumundadır.
6	Dil butonu	BMC'nin Web portalının geçerli dilini görüntüler. Dili değiştirmek için bu butona tıklayın.
7	Geçerli kullanıcı	Mevcut durumda oturum açmış olan kullanıcıyı görüntüler. • Mevcut durumda oturum açmış olan kullanıcının, IP adresi ve oturum açma zamanı dahil ayrıntılarını görmek için bu butona tıklayın. • Mevcut durumda oturum açmış olan kullanıcının oturumunu kapatmak için bu butona tıklayın ve daha sonra görüntülenen ayrıntılı bilgi kutusu içerisinde **Log Out** üzerine tıklayın.

8	**Shortcuts**	BMC'nin Web portalındaki kısayol işlem butonlarını görüntüler; bunlar aşağıdaki gibidir; • **Firmware Upgrade**: firmware'i (donanım yazılımı) yükseltir. Detaylar için 8.4 Firmware'ın Yükseltilmesi bölümüne başvurun. • **Log**: BMC loglarını sorgular. Detaylar için, 6.6 BMC Loglarının Sorgulanması bölümüne başvurun. • **Network**: ağ parametrelerini yapılandırır. Detaylar için 8.1 Ağ Parametresi Konfigürasyonu bölümüne başvurun. • **Power**: sunucu açık/kapalı bilgisini ve güç kaynağı ve güç tüketimi bilgilerini sorgular. Detaylar için 5.6 Sunucunun Açılması/Kapatılması ve 5.12 Güç Kontrolü Parametrelerinin Yapılandırılması bölümüne başvurun. • **One-Click Collection**: Arıza yeri belirleme için tüm konfigürasyon dosyalarını, veritabanlarını ve logları toplar, bunları paketler ve PC'ye indirir. Gerekli bilgilerin toplanması uzun zaman alır ve toplama süresi boyunca diğer başka işlemler gerçekleştirilemez.

No.	Ad	Açıklama
9	**Device List**	Sunucu içerisindeki bileşenleri kategoriye göre görüntüler. Bir kategorinin bileşenlerinin ayrıntılarını görüntülemek için o kategori üzerine tıklayın.
10	**Virtual Console**	Sanal konsol ile ilgili işlemleri görüntüler, bu işlemler aşağıdakileri içerir: • **Virtual Console** alanında KVM önizlemesini etkinleştirmek için **Open Preview** üzerine tıklayın. • **Virtual Console** alanında KVM önizlemesinin etkinliğini kaldırmak için **Close Preview** üzerine tıklayın. • Sanal konsolu, HTML modunda başlatmak için **Operate** üzerine tıklayın ve ardından kısayol menüsünden **Start HTML Virtual Console** seçimini yapın. • Sanal konsolu, Java modunda başlatmak için **Operate** üzerine tıklayın ve ardından kısayol menüsünden **Start Java Virtual Console** seçimini yapın. • Sanal konsolu sıfırlamak için **Operate** üzerine tıklayın ve ardından kısayol menüsünden **Reset Virtual Console** seçimini yapın. • **Settings** üzerine tıklayın.
11	**System Monitoring**	Sistem izleme bilgilerini görüntüler.

Bölüm 4
Genel İşlemler

İçindekiler Tablosu

4.1 SSH Üzerinden BMC'de Oturum Açma

Özet

Bu prosedürde BMC'yi yapılandırmak için SSH üzerinden BMC'de nasıl oturum açılacağını açıklanmıştır.

Önkoşul

PC'ye halihazırda SSH yazılımı yüklenmiş olmalıdır, örneğin; *PuTTY*.

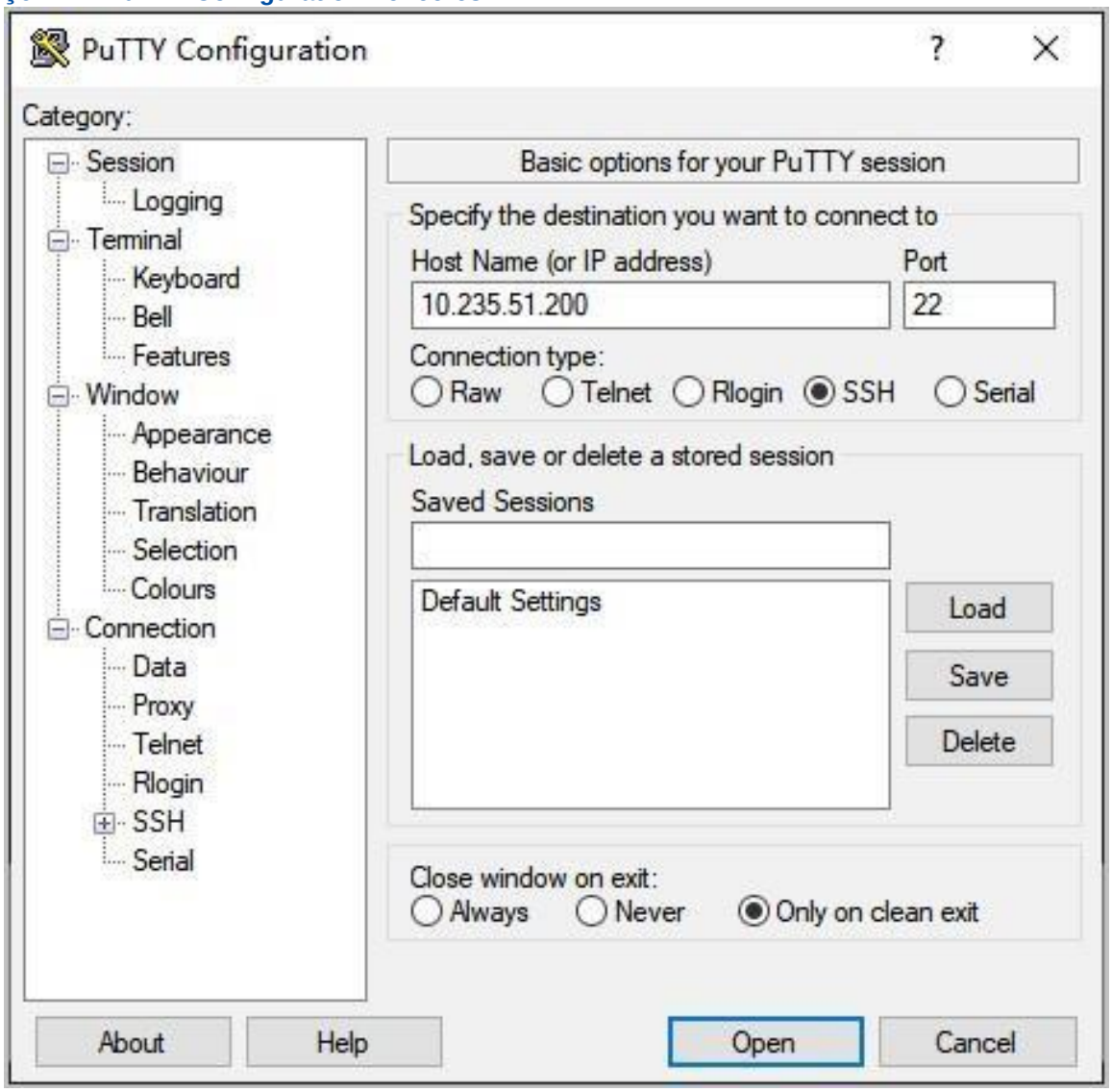
Not

Farklı SSH yazılımları için uygulanan işlemler benzerdir. Bu prosedürde örnek olarak *PuTTY* yazılımı kullanılmıştır.

Adımlar

1. PC'de *PuTTY* yazılımını başlatın. **PuTTY Configuration** penceresi görüntülenir, bakınız Şekil 4-1.

Şekil4-1 PuTTY Configuration Penceresi



2. Parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 4-1'e başvurun.

Tablo 4-1 PuTTY Configuration Parametre Açıklamaları

Parametre	Ayarlar
Category	**Session**'ı seçin.
Host Name (or IP address)	iSAC yönetim ağ portunun veya paylaşılan ağ portunun IP adresini girin.

Port	*22* girin.
Parametre	**Ayarlar**
Connection type	**SSH'yi** seçin.

3. **Open** üzerine tıklayın. CLI görüntülenir.
4. Sistem yöneticisinin (admin) kullanıcı adını ve parolasını girin.

Not

Sistem yöneticisi için varsayılan hesap *sysadmin*'dir ve varsayılan parola sürüme bağlıdır:

- V04.23.01.02'den önceki sürümler için: superuser
- V04.23.01.02'den sonraki sürümler için: Superuser@123

Not

Varsayılan parolayı kullanarak BMC yönetim sisteminde oturum açtıktan sonra varsayılan kullanıcı parolasını derhal değiştirin. Parolayı güçlü bir parola ile değiştirmeniz önerilir.

5. BMC'de oturum açmak için **Enter'a** basın.

4.2 Bir Seri Port Üzerinden BMC'de Oturum Açma

Özet

BMC'ye erişim için ne iSAC yönetim ağ portu ne de paylaşılan ağ portu kullanılabilir olmadığında, BMC'yi yapılandırmak üzere bir seri port üzerinden BMC'de oturum açabilirsiniz.

Önkoşul

- PC'ye halihazırda SSH yazılımı yüklenmiş olmalıdır, örneğin; *PuTTY* .

Not

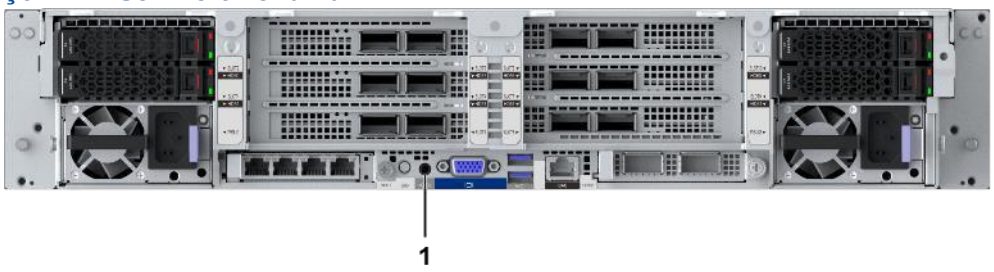
Farklı SSH yazılımları için uygulanan işlemler benzerdir. Bu prosedürde örnek olarak *PuTTY* yazılımı kullanılmıştır.

- PC'nin bir USB portunu bir seri porta dönüştürmesi gerekliyse, ilgili sürücünün kurulu olması gereklidir.
- Bir seri kablo mevcut olmalıdır.

Adımlar

2. Bir seri kablo kullanarak sunucunun arka panelindeki seri portu PC'ye bağlayın. Arka paneldeki seri port konumu için Şekil 4-2'ye başvurun.

Şekil 4-2 Seri Port Konumu



1. Seri port

Not

Bir sunucunun arka panelindeki  bilgi etiketli port, seri portu belirtir. Bu prosedürde seri portun konumunu açıklamak için örnek olarak bir NCS6722 N4 sunucusu kullanılmıştır.

2. Sunucunun ön panelindeki UID butonuna basın ve altı saniye boyunca basılı tutun. Seri port, BMC seri port devreye alma moduna geçecektir.

Ön paneldeki UID butonunun konumu için Şekil 4-3'e başvurun.

Şekil 4-3 UID Butonunun Konumu

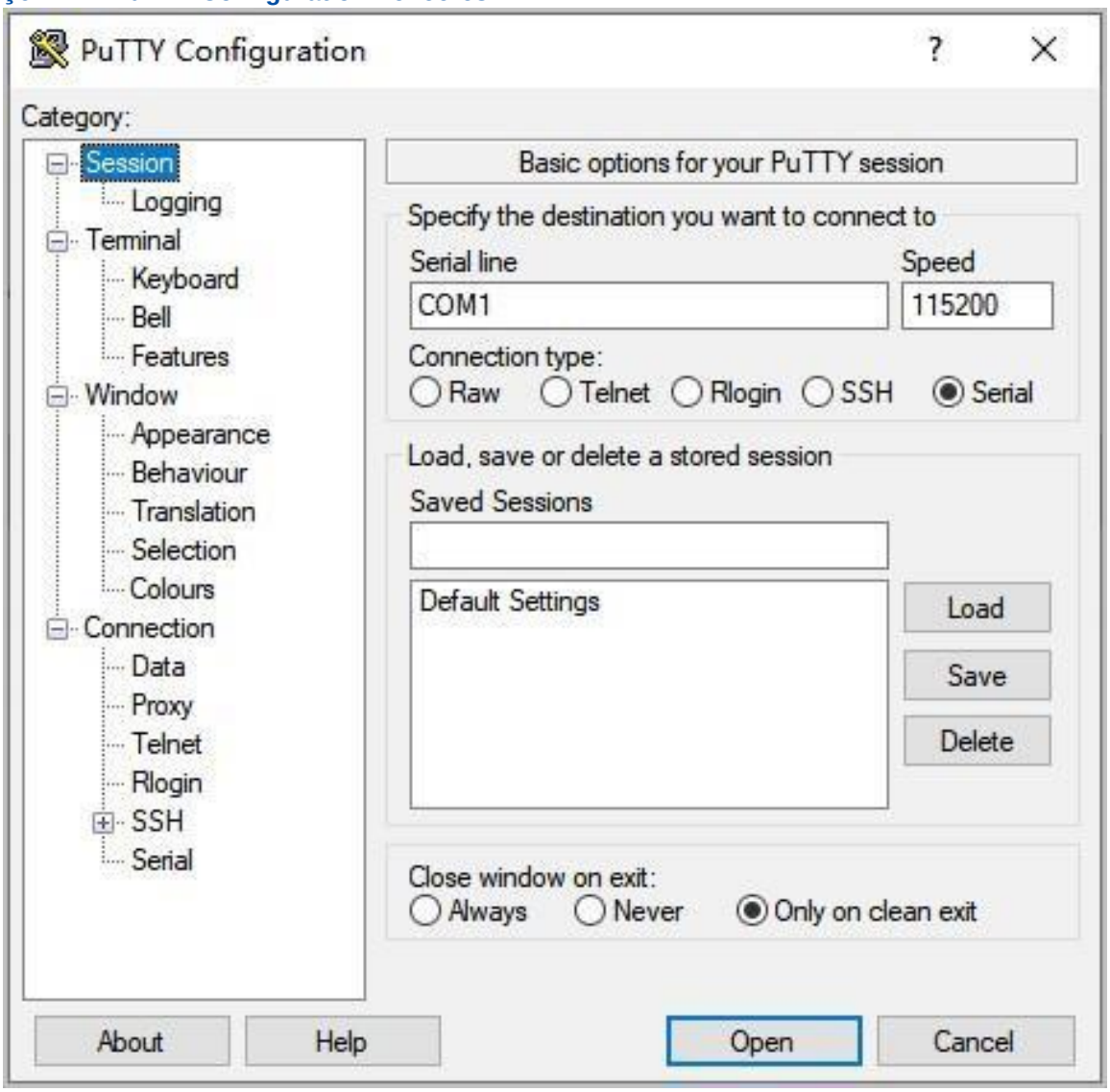
1. UID butonu

Not

Bir sunucunun ön panelindeki **UID** bilgi etiketli buton, bir UID butonudur. Bu prosedürde UID butonunun konumunu açıklamak için örnek olarak bir NCS6722 N4 sunucusu kullanılmıştır.

3. PC'deki **Device Manager** penceresi içerisinde seri kablo ile bağlanmış olan seri portu kontrol edin.
4. PC'de `PuTTY` yazılımını başlatın. **PuTTY Configuration** penceresi görüntülenir, bakınız Şekil 4-4.

Şekil 4-4 PuTTY Configuration Penceresi



5. Parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 4-2'ye başvurun.

Tablo 4-2 PuTTY Configuration Parametre Açıklamaları

Parametre	**Ayarlar**
Category	**Session**'ı seçin.
Serial line	Adım 3'te elde ettiğiniz seri portu girin.
Speed	*115200* girin.
Connection type	**Serial** seçin.

6. **Open** üzerine tıklayın. CLI görüntülenir.
7. Sistem yöneticisinin (admin) kullanıcı adını ve parolasını girin.

Not

Sistem yöneticisi için varsayılan hesap *sysadmin*'dir ve varsayılan parola sürüme bağlıdır:

- V04.23.01.02'den önceki sürümler için: superuser
- V04.23.01.02'den sonraki sürümler için: Superuser@123

Not

Varsayılan parolayı kullanarak BMC yönetim sisteminde oturum açtıktan sonra varsayılan kullanıcı parolasını derhal değiştirin. Parolayı güçlü bir parola ile değiştirmeniz önerilir.

8. BMC'de oturum açmak için **Enter'a** basın.

4.3 BMC Adresinin Değiştirilmesi

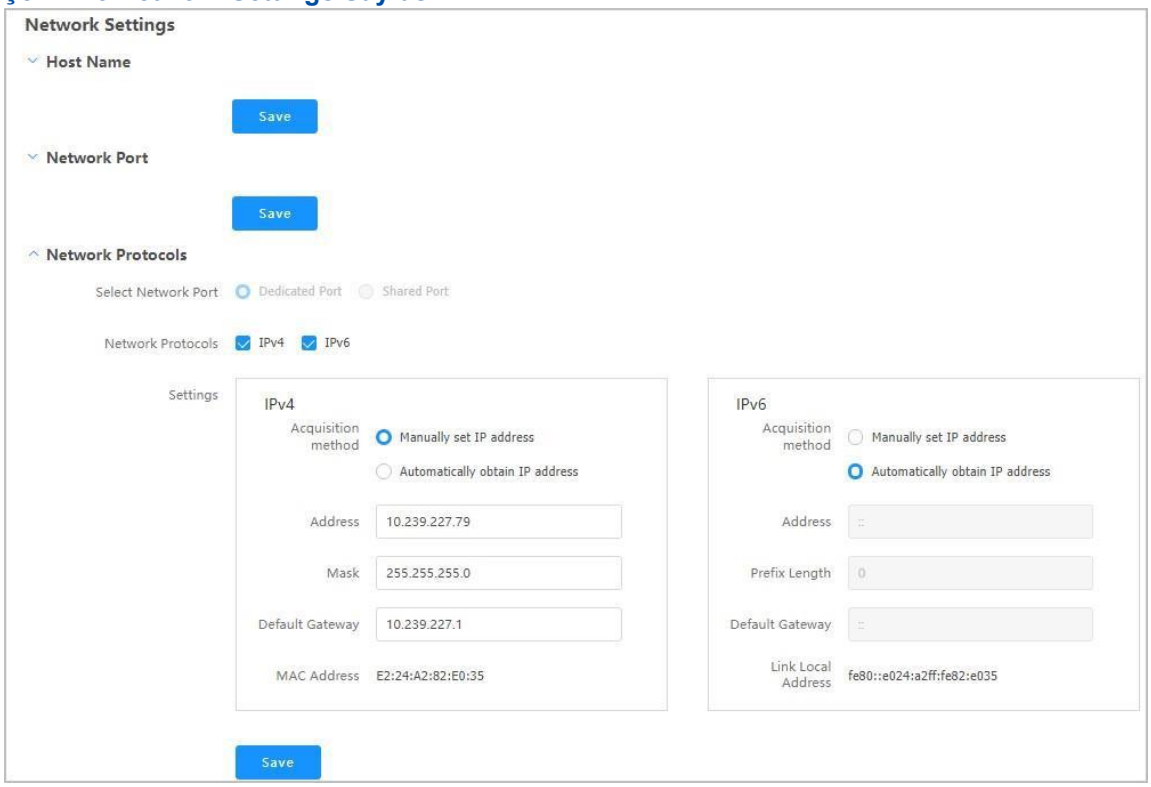
Özet

iSAC yönetim ağ portunun veya paylaşılan ağ portunun IP adresini yeniden planlamak için BMC'nin adresini değiştirmeniz gerekir.

Adımlar

1. **BMC Settings'i** seçin. **BMC Settings** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Network Settings** seçimini yapın. **Network Settings** sayfası görüntülenir, bakınız Şekil 4-5.

Şekil 4-5 Network Settings Sayfası



3. **Network Protocols** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 4-3'e başvurun.

Tablo 4-3 Network Protocol Parametre Açıklamaları

Parametre	**Ayarlar**
Select Network Port	Bu parametre sadece Network Port alanında **Select Mode**, **Alone** olarak ayarlandığında ayarlanabilir . Bir IP adresini yapılandırmak istediğiniz ağ portunu seçin. • **Dedicated Port**: iSAC yönetim ağ portunun IP adresini yapılandırır. • **Shared Port**: paylaşılan ağ portunun IP adresini yapılandırır.
Network Protocols	Ağ portu için ağ protokolünü(lerini) seçin. • Sadece **IPv4** seçmeniz durumunda IPv4 ayarlarının yapılandırılması gerekir. • Sadece **IPv6** seçmeniz durumunda IPv6 ayarlarının yapılandırılması gerekir. • **IPv4** ve **IPv6** seçmeniz durumunda hem IPv4 hem de IPv6 ayarlarının yapılandırılması gerekir.
Acquisition method	Bir IP adresi alma yöntemi seçin. **Acquisition method** değeri **Automatically obtain IP address** olarak ayarlandığında aşağıdaki parametrelerin yapılandırılması gerekmez.

Address	Planlandığı gibi BMC'nin IP adresini girin.
Mask	Maskeyi girin.
Parametre	**Ayarlar**
Default Gateway	Varsayılan Ağ Geçidi'nin IP adresini girin.

4. **Save** üzerine tıklayın.

4.4 Sunucu Bilgilerinin Kontrol Edilmesi

Özet

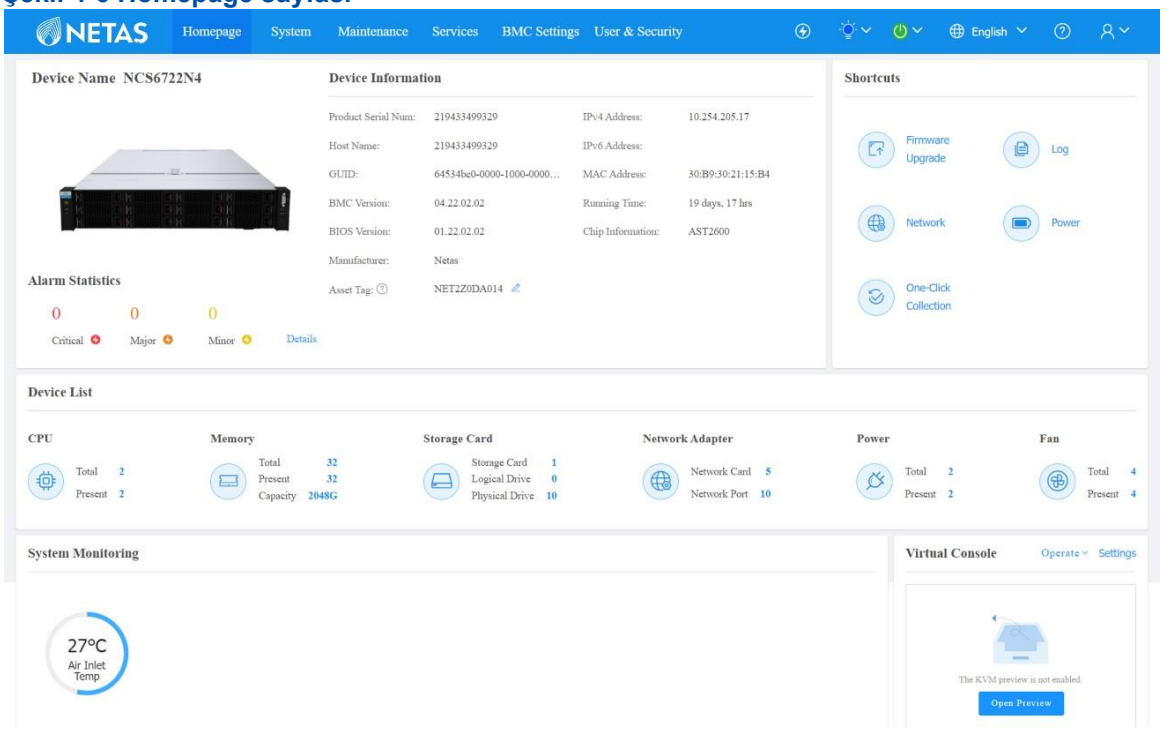
Bir arızayı raporlamadan veya donanımı değiştirmeden önce, aşağıdakiler dahil sunucu bilgilerini kontrol etmeniz gerekir:

- Seri numarası
- CPU
- Bellek
- NIC

Adımlar

1. **Homepage** sayfasında, sunucunun seri numarasını kontrol edin, bakınız Şekil 4-6.

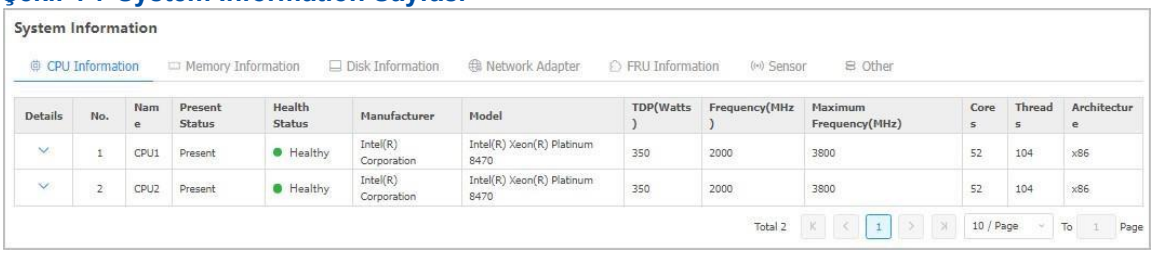
Şekil 4-6 Homepage sayfası



2. **System** seçin. **System** sayfası görüntülenir.

3. Sol taraftaki navigasyon ağacından, **System Information** seçimini yapın. **System Information** sayfası görüntülenir, bakınız Şekil 4-7.

Şekil 4-7 System Information Sayfası



- CPU bilgisini kontrol etmek için **CPU Information** sekmesine geçin.
- Bellek bilgisini kontrol etmek için **Memory Information** sekmesine geçin.
- NIC bilgisini kontrol etmek için **Network Adapter** sekmesine geçin.

4.5 Depolama Cihazlarının Yönetilmesi

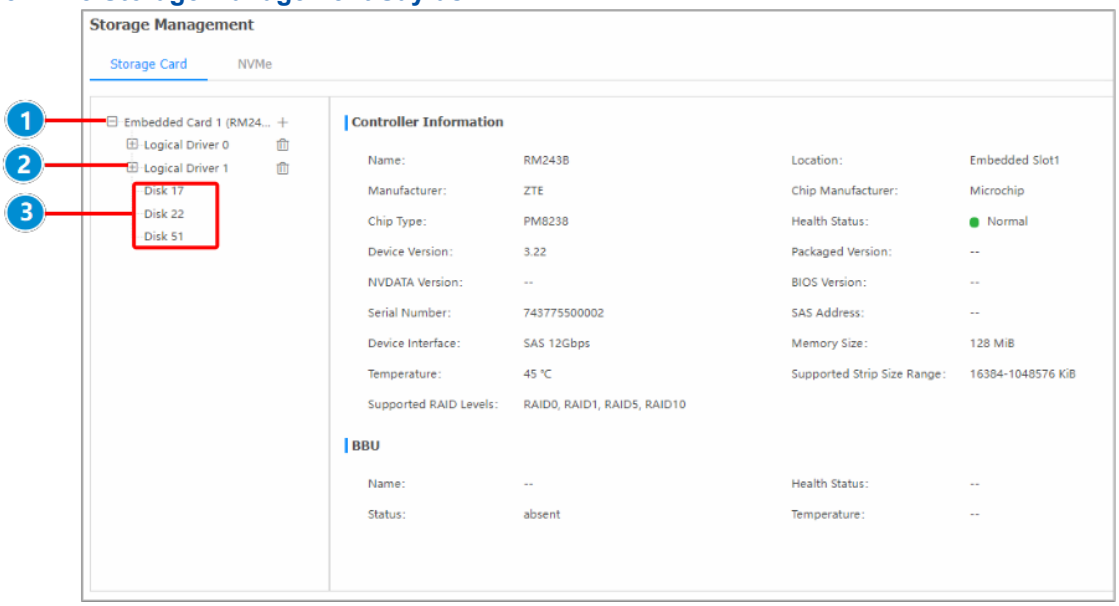
Özet

Bir sunucunun depolama cihazları; RAID denetleyicilerini ve sabit diskleri ifade eder.
Bir RAID denetleyicisi tarafından yönetilen fiziksel diskler, mantıksal diskler olarak oluşturulabilir.
Sabit diskler arayüz türüne göre SAS diskleri ve NVMe diskleri olarak sınıflandırılabilirler.
Storage Management sayfasındaki **Storage Card** sekmesi, SAS disklerini ve **NVMe** sekmesi de NVMe disklerini görüntüler.

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Storage Management** seçimini yapın. **Storage Management** sayfası görüntülenir, bakınız Şekil 4-8.

Şekil 4-8 Storage Management Sayfası



1. RAID denetleyici
2. Mantıksal disk
3. Fiziksel disk

3. Aşağıdaki işlemleri gerektiği gibi gerçekleştirin.

Aşağıdakileri gerçekleştirmek için...	**Şunları yapınız...**
RAID denetleyicisi ve BBU bilgilerinin kontrol edilmesi	**Storage Card** sekmesinde istediğiniz RAID denetleyicisine tıklayın. RAID denetleyicisi ve BBU bilgileri sağ tarafta görüntülenir.
Mantıksal disk bilgilerinin kontrol edilmesi	**Storage Card** sekmesinde istediğiniz mantıksal diske tıklayın. Detaylı mantıksal disk bilgisi sağ tarafta görüntülenir. Mantıksal disk bilgisinde **Status** aşağıdakileri içerir: • **Optimal** • **Degraded** • **Part Degraded** • **Offline**
Bir mantıksal diskin UID göstergesinin ayarlanması.	a. **Storage Card** sekmesinde istediğiniz mantıksal diske tıklayın. b. Sağ taraftaki **Settings** üzerine tıklayın. **Logical Drive Setting** iletişim kutusu görüntülenir. c. **Open** ya da **Close** seçin. • **Open**: mantıksal diskin tüm üye disklerinin UID göstergelerini açar. • **Off**: mantıksal diskin tüm üye disklerinin UID göstergelerini kapatır. d. **Submit** üzerine tıklayın.

Fiziksel disk bilgilerinin kontrol edilmesi	**Storage Card** sekmesinde istediğiniz fiziksel diske tıklayın. Detaylı fiziksel disk bilgisi sağ tarafta görüntülenir.
Aşağıdakileri gerçekleştirmek için...	**Şunları yapınız...**
Bir mantıksal diskin oluşturulması	a. **Storage Card** sekmesinde RAID denetleyicisinin yanındaki **+** simgesine tıklayın. Sağ tarafta **Create Logical Drive** alanı görüntülenir, bakınız Şekil 4-9. b. Aşağıdaki parametreleri yapılandırın: • **Logical disk name**: Mantıksal diskin adını girin. • **RAID Level**: İlgili RAID seviyesini seçin. • **Stripe Size**: Bir stripe size değeri girin. • **Physical Drive Configuration**: Mantıksal diski oluşturan üye diskleri seçin. c. **Save** üzerine tıklayın.
NVMe sabit disk bilgilerinin sorgulanması	**Storage Management** sayfasında, **NVMe** sekmesine geçmek için **NVMe** üzerine tıklayın. Detaylı NVMe disk bilgisi görüntülenir.

Şekil 4-9 Create Logical Drive Alanı

Not

Mantıksal diskleri oluşturmak için farklı RAID denetleyici türlerinin farklı sayfaları vardır.

4.6 İşletim Sisteminin (OS) Uzaktan Yüklenmesi

Özet

Müşteri sahasında olmadığınızda, bir sunucu için İşletim Sistemini (OS) bir PC üzerinden uzaktan yükleyebilirsiniz.

Uzaktan İşletim Sistemi kurulumu için yapılacak işlemler aşağıdakileri içerir:

1. Ortam yeniden yönlendirme konfigürasyonlarının devre dışı bırakılması
2. Bir önyükleme (boot) modunun yapılandırılması
3. Bir İşletim Sisteminin yüklenmesi

Önkoşul

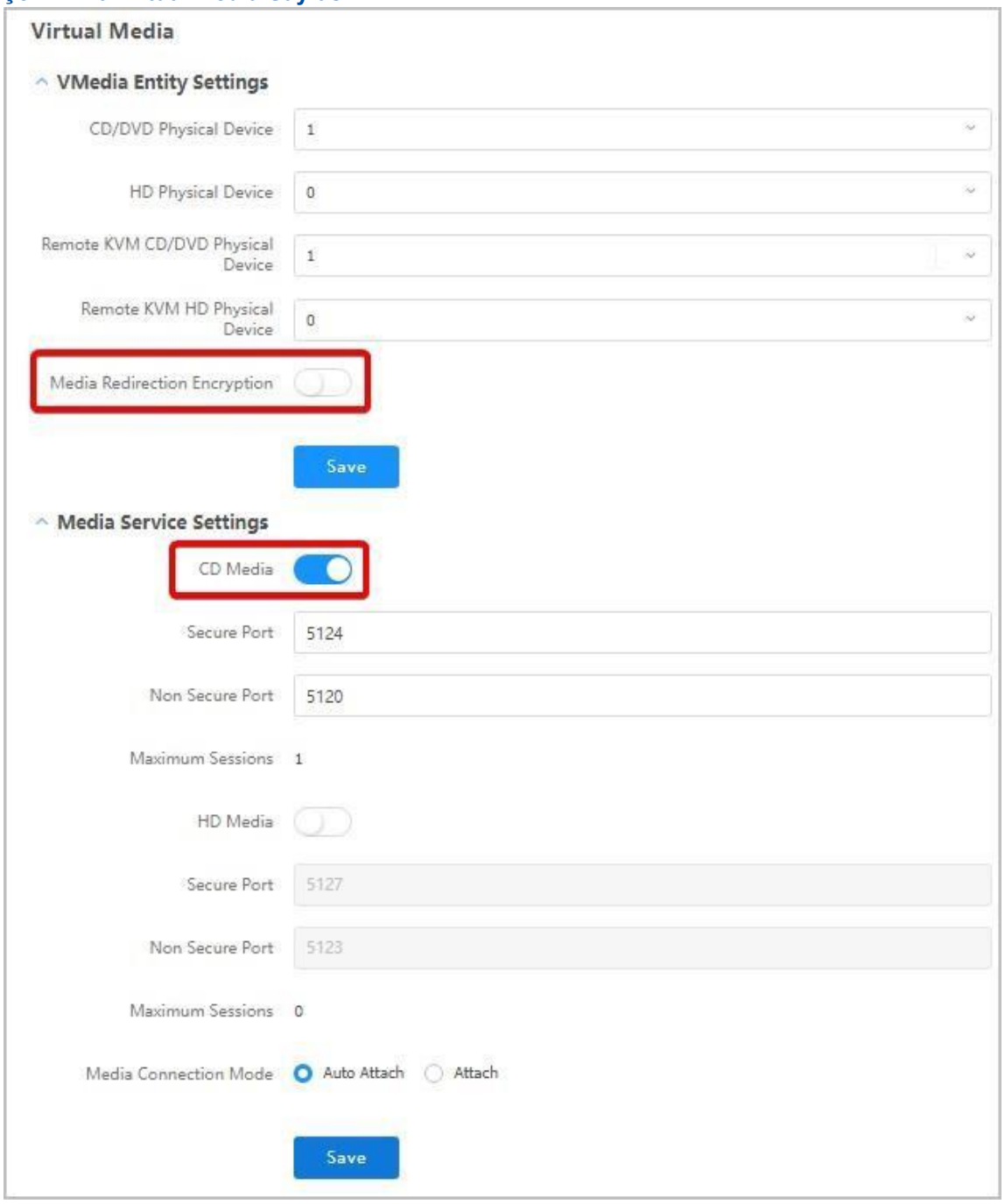
- İşletim Sisteminin *iso* dosyası halihazırda alınmış olmalıdır.
- Sunucunun sistem diskinin RAID konfigürasyonu halihazırda tamamlanmış olmalıdır.
- Eğer KVM'nin Java modunda başlatılması gerekliyse, JRE (örneğin, *jre-8u191*) PC'ye halihazırda kurulmuş olmalıdır.

Adımlar

Ortam Yeniden Yönlendirme Konfigürasyonlarının Devre Dışı Bırakılması

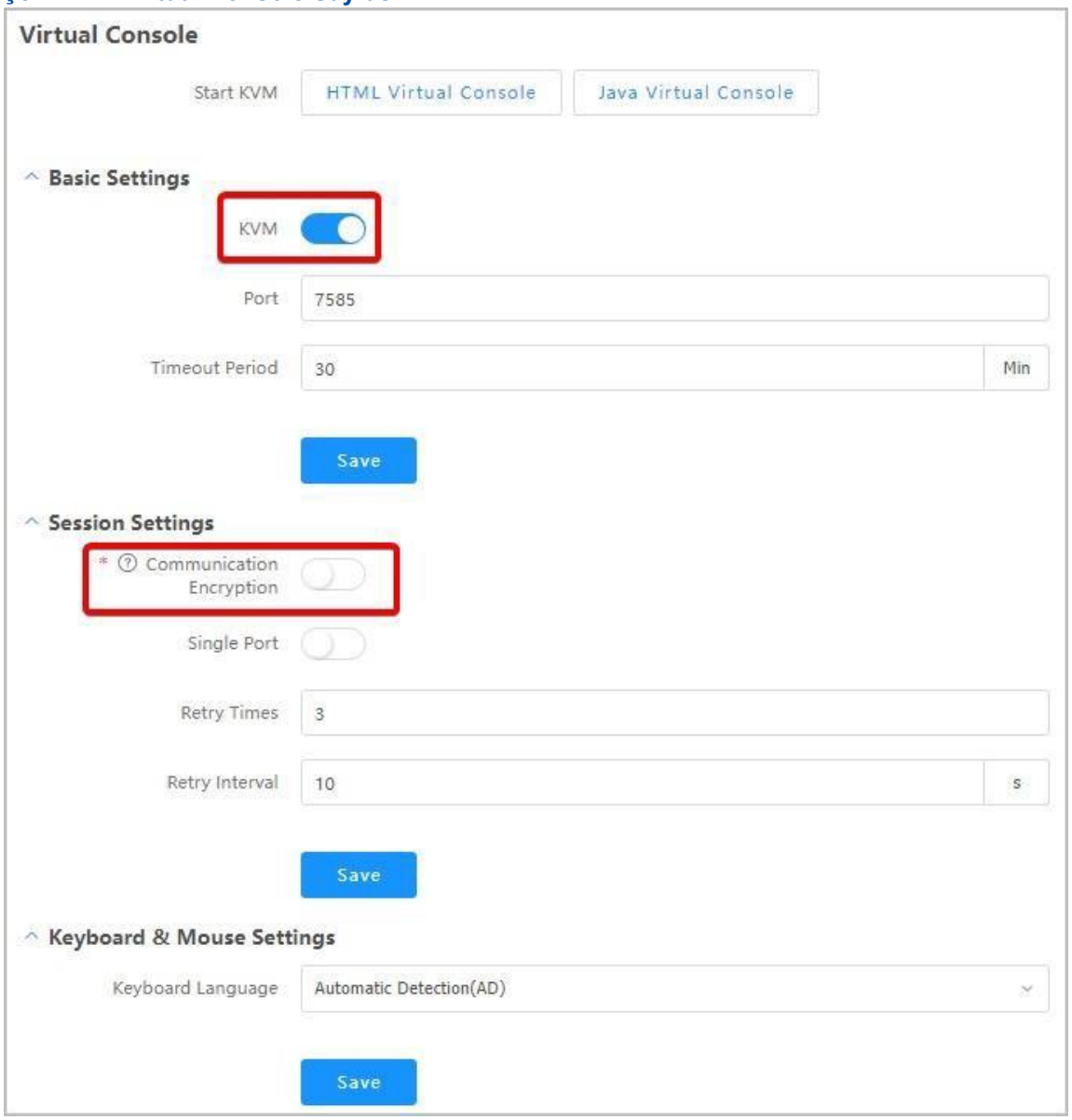
1. **Services'i** seçin. **Services** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Virtual Media** seçimini yapın. **Virtual Media** sayfası görüntülenir, bakınız Şekil 4-10.

Şekil 4-10 Virtual Media Sayfası



3. VMedia Entity Settings alanında, Media Redirection Encryption'ı kapatın ve Save üzerine tıklayın.
4. **Media Service Settings** alanında **CD Media'yı** açın ve **Save** üzerine tıklayın.
5. Sol taraftaki navigasyon ağacından, **Virtual Console** seçimini yapın. **Virtual Console** sayfası görüntülenir, bakınız Şekil 4-11.

Şekil 4-11 Virtual Console Sayfası

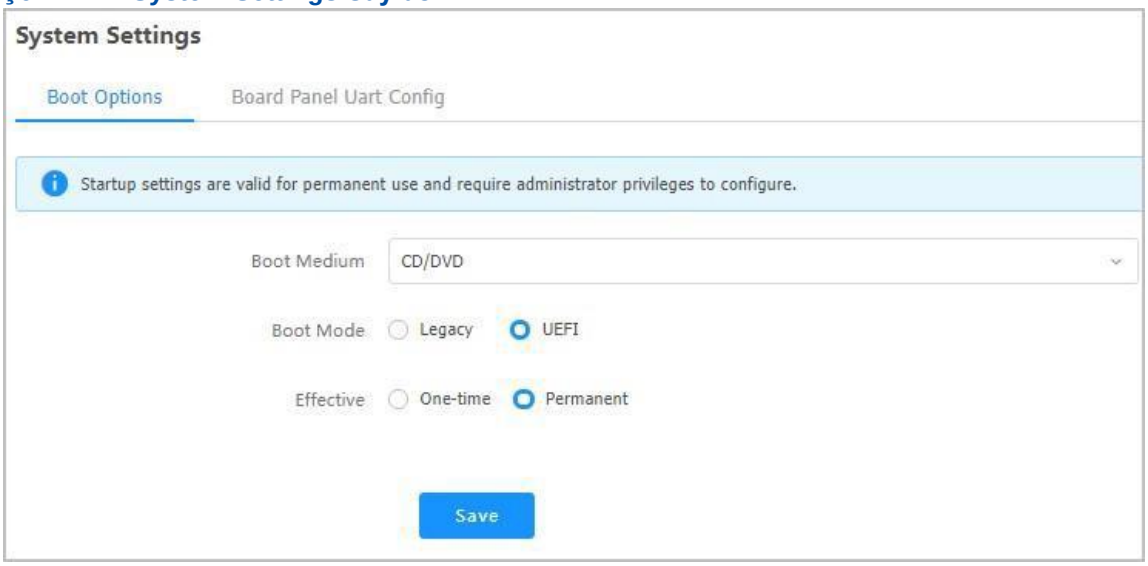


6. **Basic Settings** alanında **KVM'yi** açın ve **Save** üzerine tıklayın.
7. **Session Settings** alanında **Communication Encryption'ı** açın ve **Save** üzerine tıklayın.

Bir önyükleme (boot) modunun yapılandırılması

8. **System** seçin. **System** sayfası görüntülenir.
9. Sol taraftaki navigasyon ağacından, **System Settings** seçimini yapın. **System Settings** sayfası görüntülenir, bakınız Şekil 4-12.

Şekil 4-12 System Settings Sayfası



10. Parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 4-4'e başvurun.

Tablo 4-4 Boot Option Parametre Açıklamaları

Parametre	Ayarlar
Boot Medium	**CD/DVD'yi** seçin.
Boot Mode	**UEFI'yı** seçin.
Effective	**Permanent**'ı seçin.

11. **Save** üzerine tıklayın.

Bir İşletim Sisteminin yüklenmesi

12. **Services'i** seçin. **Services** sayfası görüntülenir.
13. Sol taraftaki navigasyon ağacından, **Virtual Console** seçimini yapın. **Virtual Console** sayfası görüntülenir.
14. Aşağıdaki işlemleri gerektiği gibi gerçekleştirin.

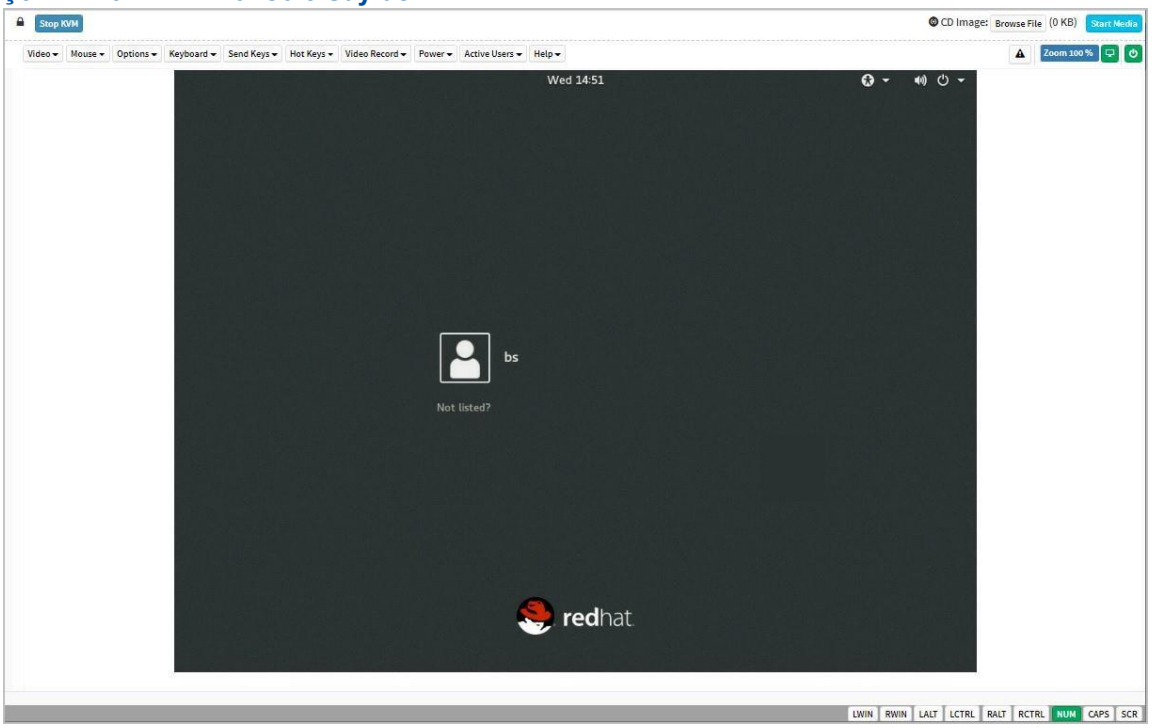
Aşağıdakileri gerçekleştirmek için...	Şunları yapınız...
KVM'nin HTML modunda başlatılması	a. **HTML Virtual Console** üzerine tıklayın. **HTML Virtual Console** sayfası görüntülenir, bakınız Şekil 4-13. b. **CD Image'nin** yanındaki **Browse File** üzerine tıklayın ve PC'den `iso` dosyasını seçin. c. `iso` dosyasını yüklemek için **Start Media** üzerine tıklayın. d. Sunucuyu yeniden başlatmak için **Power > Reset Server** seçimini yapın. İşletim Sistemini yükleme sayfası görüntülenir.

KVM'nin Java modunda başlatılması	a. PC'nin sol alt köşesindeki arama kutusuna `Java` girin. b. Arama sonuçları arasından **Configure Java'yı** seçin. **Java Control Panel** iletişim kutusu görüntülenir.
Aşağıdakileri gerçekleştirmek için...	**Şunları yapınız...**
	c. **Security** üzerine tıklayın. **Security** penceresi görüntülenir. d. **Edit Site List** üzerine tıklayın. **Exception Site List** iletişim kutusu görüntülenir. e. BMC Web portalının adresini eklemek için **Add** üzerine tıklayın. f. **Security** penceresine dönmek için **OK** üzerine tıklayın. g. **OK** üzerine tıklayın. h. BMC Web Portalının **Virtual Console** sayfasında **Java Virtual Console** üzerine tıklayın. `jviewer.jnlp'yi` saklamak isteyip istemediğinize dair bir iletişim kutusu görüntülenir. i. **Keep** üzerine tıklayın. j. Tarayıcının sol alt köşesinde `jviewer.jnlp` üzerine tıklayın. Devam etmek isteyip istemediğinize dair bir iletişim kutusu görüntülenir. k. **Continue** üzerine tıklayın. **Do you want to run this application?** iletişim kutusu görüntülenir. l. **I accept the risk and want to continue to run this app.** seçeneğini seçin ve **Run** üzerine tıklayın. **Untrusted Connection** iletişim kutusu görüntülenir. m. **Yes** üzerine tıklayın. **Java Console** sayfası görüntülenir, bakınız Şekil 4-14. **n. Media > Virtual Media Wizard...** seçimini yapın ve **CD/DVD** sekmesine geçin . o. **Browse** üzerine tıklayın ve PC'den `iso` dosyasını seçin. p. **Connect** üzerine tıklayın. q. Sunucuyu yeniden başlatmak için **Power > Reset Server** seçimini yapın. İşletim Sistemini yükleme sayfası görüntülenir.

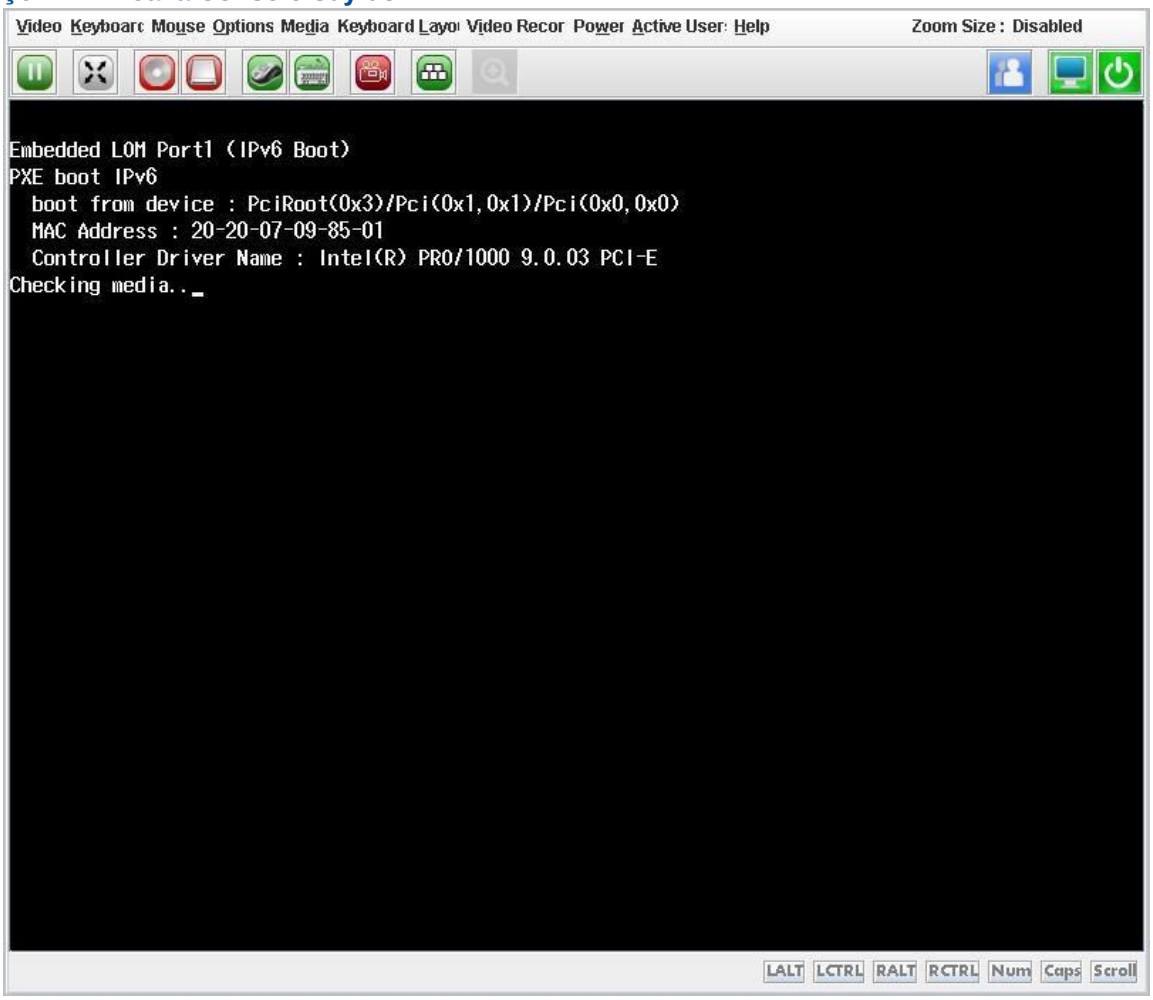
Not

KVM'yi bir modda başlatmadan önce, KVM'yi diğer modda devre dışı bırakmanız gerekir. Örneğin; KVM'yi Java modunda başlatmadan önce HTML modunda başlatılmış olan KVM'yi devre dışı bırakmanız gerekir.

Şekil 4-13 HTML Console Sayfası



Şekil 4-14 Java Console Sayfası



4.7 Web Portalı Kullanılabilir Olmadığında BMC'nin Sıfırlanması

Özet

Eğer BMC'nin Web portalında oturum açamıyorsanız, BMC'yi sıfırlamanız gerekir. BMC'yi aşağıdaki yollardan birini kullanarak sıfırlayabilirsiniz:

- BMC'nin sunucuda oturum açarak sıfırlanması
- BMC'nin bir SSH aracı (örneğin; PuTTY) kullanarak sıfırlanması
- BMC'nin ipmitool kullanarak sıfırlanması
- BMC'nin sunucuyu kapatarak sıfırlanması

Önkoşul

- BMC'yi ipmitool kullanarak sıfırlamak istemeniz durumunda, **ipmi** hizmet portu numarası halihazırda **623 olarak** ayarlanmıştır.
- BMC'yi ipmitool kullanarak sıfırlamak istemeniz durumunda, BMC adresine ipmitool yoluyla başarıyla ping atabilirsiniz.

Adımlar

- BMC'nin sunucuda oturum açarak sıfırlanması

  1. `root` kullanıcısı olarak sunucuda oturum açın.
  2. BMC'yi sıfırlamak için aşağıdaki komutları çalıştırın:

     ```
     # modprobe ipmi_si
     # modprobe ipmi_devintf
     # ipmitool mc reset cold
     ```

- BMC'nin bir SSH aracı kullanarak sıfırlanması

  1. SSH aracını kullanarak BMC'de oturum açın ve oturumun açılabilmesi için aşağıdaki parametreleri girin:

     → Host address: BMC'nin adresi

     → Username: sysadmin

     → Password: Varsayılan parola sürüme bağlıdır:
     V04.23.01.02'den önecki sürümler için: superuser

     V04.23.01.02'den sonraki sürümler için:

     Superuser@123

     Not

     Varsayılan parolayı kullanarak BMC yönetim sisteminde oturum açtıktan sonra varsayılan kullanıcı parolasını derhal değiştirin. Parolayı güçlü bir parola ile değiştirmeniz önerilir.

     → Port number: 22

  2. BMC'yi sıfırlamak için aşağıdaki komutu çalıştırın:

     ```
     # reboot
     ```

- BMC'nin ipmitool kullanarak sıfırlanması

  1. BMC'yi sıfırlamak için ipmitool'da aşağıdaki komutlardan herhangi birisini çalıştırın:

     → Warm boot: **`ipmitool -I lanplus -H 10.43.211.200 -U root -P Root12349! mc reset warm Sent warm reset command to MC`**

     → Cold boot: **`ipmitool -I lanplus -H 10.43.211.200 -U root P Root12349! mc reset cold Sent cold reset command to MC`**
     Yukarıdaki komutlar içerisindeki parametreler aşağıda açıklandığı gibidir:

     → **10.43.211.200**: BMC'nin adresi → **root**: kullanıcı adı

     → **Root12349!**: parola

- BMC'nin sunucuyu kapatarak sıfırlanması

  1. Hizmetlerin olmadığı sunucuyu kapatın.
  2. Sunucuyu açın.

4.8 Sıcaklık Politikasının Sorgulanması ve Yapılandırılması

Özet

Sıcaklık politikası, sunucunun sıcaklığı belirlenmiş olan eşik değerine ulaştıktan sonra sunucunun kapatılıp kapatılmayacağını belirler.
Bu prosedürde sıcaklık politikasının ipmitool kullanılarak nasıl sorgulanacağı ve yapılandırılacağı açıklanmıştır.

Adımlar

1. Sıcaklık politikasını sorgulamak için ipmitool'da şu komutu çalıştırın: **`ipmitool -I lanplus -H 10.43.211.200 -U root -P root12349! raw 0x2e 0xd6 0x3e 0x0f 0`**

Komut içerisindeki parametreler aşağıda açıklandığı gibidir:

- **10.43.211.200**: BMC'nin IP adresi
- **root**: kullanıcı adı ● **root12349!**: parola

Komut çıktısı olarak dönen değerler aşağıda açıklandığı gibidir:

- **1**: aşırı sıcaklık kapatma politikasının etkinleştirilmiş olduğunu belirtir.
- **0**: aşırı sıcaklık kapatma politikasının devre dışı bırakılmış olduğunu belirtir.

2. (Opsiyonel) Sıcaklık politikasını değiştirmek için şu komutu çalıştırın: **`ipmitool -I lanplus -H 10.43.211.200 -U root -P root12349! raw 0x2e 0xd6 0x3e 0x0f 0 1`**

Komuttaki son byte aşağıda açıklandığı gibidir:

- **1**: aşırı sıcaklık kapatma politikasını etkinleştirir.
- **0**: aşırı sıcaklık kapatma politikasını devre dışı bırakır.

4.9 Hizmetlerin Sorgulanması ve Yapılandırılması

Özet

Varsayılan olarak BMC aşağıdaki hizmetleri sağlar:

- **web**: platformdan bağımsız, az bağlantılı, kendi kendine yeten, programlanabilir web tabanlı bir uygulamadır. Bu gibi uygulamaları tanımlamak, yayınlamak, keşfetmek, koordine etmek ve yapılandırmak için dağıtık ve birlikte çalışabilir uygulamaları geliştirmek için kullanılan open XML standartlarını kullanabilirsiniz.
- **kvm**: Bir klavye, ekran veya fare aracılığıyla birden fazla cihazı kontrol eder, bunlar arasında geçiş yapar ve yönetir ve aynı zamanda uzaktan zamanlama ve izlemede önemli bir rol oynar.
- **Cd-media:** bir KVM hedef sunucusunun bir PC'deki fiziksel CD/DVD cihazlarındaki dosyalara erişmesine izin veren bir sanal ortam hizmetidir (istemci görevi görür).

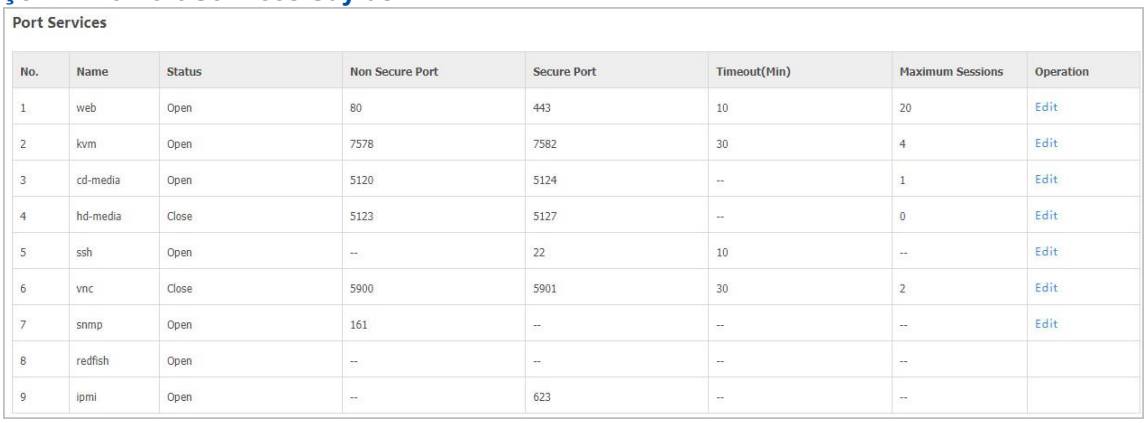
- **hd-media**: bir KVM hedef sunucusunun bir PC'deki fiziksel HD cihazlarındaki dosyalara erişmesine izin veren bir sanal ortam hizmetidir (istemci görevi görür).
- **ssh**: güvenli olmayan bir ağda, güvenli uzaktan erişim ve diğer güvenli ağ hizmetlerini sağlayan bir protokoldür.
- **vnc**: istemcinin uygulama programı (vnc görüntüleyici) ve sunucunun uygulama programından (vncserver) meydana gelen bir uzaktan kontrol aracıdır.
- **snmp**: TCP/IP ağlarında geniş çapta kullanılan bir standart ağ yönetimi protokolüdür. Farklı üreticilerin cihazlarının birleşik yönetimini sağlamak amacıyla birleşik arayüzler sağlar.
- **redfish** bir sunucu yönetim özelliğidir. Redfish Ölçeklenebilir Platformlar Yönetim API'sı ("Redfish"), bant dışı sistem yönetimi gerçekleştirmek üzere model biçiminde tanımlanan verilere erişmek için RESTful arayüzü anlambilimini kullanır. Büyük ölçekli sunucu bulut ortamlarının yönetimi ve dağıtımı/konuşlandırılması için uygundur.
- **ipmi**: sunucu yönetim sistemi tasarımına uygulanan bir standarttır.

Bu prosedürde yukarıda belirtilen hizmetlerin parametrelerinin nasıl sorgulanacağı ve değiştirileceği açıklanmıştır.

Adımlar

1. **Services'i** seçin. **Services** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Port Services** seçimini yapın. **Port Services** sayfası görüntülenir, bakınız Şekil 4-15.

Şekil 4-15 Port Services Sayfası


Port Services

No.	Name	Status	Non Secure Port	Secure Port	Timeout(Min)	Maximum Sessions	Operation
1	web	Open	80	443	10	20	Edit
2	kvm	Open	7578	7582	30	4	Edit
3	cd-media	Open	5120	5124	--	1	Edit
4	hd-media	Close	5123	5127	--	0	Edit
5	ssh	Open	--	22	10	--	Edit
6	vnc	Close	5900	5901	30	2	Edit
7	snmp	Open	161	--	--	--	Edit
8	redfish	Open	--	--	--	--	
9	ipmi	Open	--	623	--	--	

3. Parametreleri etkinleştirmek üzere bir hizmet için **Edit** üzerine tıklayın.
4. Parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 4-5'e başvurun.

Tablo 4-5 Port Service Parametre Açıklamaları

Parametre	Ayarlar
Status	Bir hizmetin etkinleştirilip etkinleştirilmeyeceğini seçin.

Non Secure Port	Hizmetin güvenli olmayan port numarasını girin. • Web hizmetinin güvenli olmayan varsayılan port numarası: 80. • KVM hizmetinin güvenli olmayan varsayılan port numarası: 7578. • CD ortam/medya hizmetinin varsayılan güvenli olmayan port numarası: 5120. • HD ortam/medya hizmetinin varsayılan güvenli olmayan port numarası: 5123. • VNC hizmetinin güvenli olmayan varsayılan port numarası: 5900. • SNMP hizmetinin güvenli olmayan varsayılan port numarası: 161. Diğer hizmetler güvenli olmayan portları desteklemez. Güvenli olmayan port numarası aralığı: 1–65535.
Secure port	Hizmetin güvenli port numarasını girin. • Web hizmetinin varsayılan güvenli port numarası: 443. • KVM hizmetinin varsayılan güvenli port numarası: 7582. • CD ortam/medya hizmetinin varsayılan güvenli port numarası: 5124. • HD ortam/medya hizmetinin varsayılan güvenli port numarası: 5127. • SSH hizmetinin varsayılan güvenli port numarası: 22. • VNC hizmetinin varsayılan güvenli port numarası: 5901. • IPMI hizmetinin varsayılan güvenli port numarası: 623. Diğer hizmetler güvenli portları desteklemez. Güvenli port numarası aralığı: 1–65535.
Timeout(Min)	Belirlenen zaman aşımı süresi içinde hiçbir işlem yapılmazsa hizmet sonlandırılır. Zaman aşımı süresini (dakika cinsinden) girin. Aralık: 5–30 (VNC hizmeti için) veya 1–30 (diğer hizmetler için).

Not

Maximum Sessions parametresini yapılandıramazsınız.

5. **Save**

Doğrulama

- Redfish hizmetini etkinleştirdikten sonra, Redfish arayüzü üzerinden BMC'yi sorgulayabilir ve yapılandırabilirsiniz.

  Redfish arayüzü hakkında detaylı açıklama için, `NETAŞ Server Redfish Interface Description (BMC V4)` dokümanına başvurun. `NETAŞ Server Redfish Interface Description (BMC V4)` dosyasını nasıl alabileceğiniz hakkında bilgi almak için 10 Referans: Dokümanlara Erişim bölümüne başvurun. .

- SNMP hizmetini etkinleştirdikten ve doğru bir güvenli olmayan port yapılandırdıktan sonra, SNMP arayüzü üzerinden BMC'yi sorgulayabilir ve yapılandırabilirsiniz.

SNMP arayüzü hakkında detaylı açıklama için, `NETAŞ Server SNMP Interface Description (BMC V4)` dokümanına başvurun.

`.NETAŞ Server SNMP Interface Description (BMC V4)` dosyasını nasıl alabileceğiniz hakkında bilgi almak için 10 Referans: Dokümanlara Erişim bölümüne başvurun. .

4.10 NTP Sunucusunun Yapılandırılması

Özet

NTP sunucusu, BMC'nin zaman senkronizasyonu kaynağıdır. Eğer BMC'nin zamanının NTP sunucusundan senkronize edilmesi gerekiyorsa, NTP sunucusunu yapılandırmanız gereklidir.

NTP sunucusunu yapılandırmak için aşağıdaki işlemleri gerçekleştirin:

1. NTP hizmetinin etkinleştirilmesi: zamanının senkronize edilmesi gereken cihazlar için NTP hizmeti sağlar.
2. Registry'nin (kayıt) değiştirilmesi: NTP hizmeti ile ilgili registry parametrelerini değiştirir.
3. NTP hizmetinin yeniden başlatılması: değiştirilen registry parametrelerini uygular.

Not

Bu prosedürde, Windows Server 2012 R2 İşletim Sistemine sahip olan bir PC üzerinde gerçekleştirilen işlemler örnek olarak alınmıştır. Başka Windows Server İşletim Sistemine sahip PC'lerde gerçekleştirilecek işlemler de benzerdir.

Adımlar

NTP Hizmetinin Etkinleştirilmesi

1. Masaüstünde **This PC** üzerine sağ tıklayın ve kısayol menüsünden **Manage**'yi seçin. **Computer Management** penceresi görüntülenecektir.
2. Sol taraftaki navigasyon ağacından, **Services and Applications > Services** seçimini yapın. **Services** penceresi görüntülenir.
3. Hizmet listesi içerisinde **Windows Time** üzerine sağ tıklayın ve kısayol menüsünden **Start**'ı seçin.

Kaydın (Registry) Değiştirilmesi

4. **Windows+R**'ye basın. **Run** iletişim kutusu görüntülenir.
5. **Open** metin kutusunda, *regedit* girin ve **OK'e** tıklayın. **Registry Editor** penceresi görüntülenir.
6. Registry parametrelerini değiştirin. Parametrelerin açıklamaları için, Tablo 4-6'ya başvurun.

Tablo 4-6 Registry Parametre Açıklamaları

Registry Yolu	Parametre	Değer
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config	AnnounceFlags	5
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer	Enabled	1
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Parameters	Type	NTP

NTP Hizmetinin Yeniden Başlatılması

7. **Open** metin kutusunda, **Run** iletişim kutusunda, *cmd* girin ve **OK**'e tıklayın. Komut satırı penceresi görüntülenir.
8. NTP hizmetini durdurmak için aşağıdaki komutu çalıştırın:
   C:\> net stop w32time
9. NTP hizmetini başlatmak için aşağıdaki komutu çalıştırın:
   C:\> net start w32time
10. NTP hizmetinin başarıyla yapılandırılmış olduğunu doğrulamak için aşağıdaki komutu çalıştırın:
    C:\> w32tm /stripchart /computer:127.0.0.1
    Komut yürütüldükten sonra çıktı süresi görüntülenirse, bu yapılandırmanın başarıyla gerçekleştirilmiş olduğunu belirtir.

4.11 SMTP Sunucusunun Yapılandırılması

Özet

SMTP sunucusu BMC'den alarmları alır.

SMTP sunucusunu yapılandırmak için aşağıdaki işlemleri gerçekleştirin:

1. SMTP sunucusunun kurulması: BMC için SMTP hizmeti sağlar.
2. IP adresi ve port numarasının yapılandırılması: SMTP sunucusunun IP adresi ve port numarası BMC'nin Web portalında yapılandırıldıktan sonra, SMTP sunucundaki varsayılan yola (*C:\inetpub\mailroot\Drop*) (eğer varsa) alarm e-postaları gönderir.

Not

Bu prosedürde, Windows Server 2012 R2 İşletim Sistemine sahip olan bir PC üzerinde gerçekleştirilen işlemler örnek olarak alınmıştır. Başka Windows Server İşletim Sistemine sahip PC'lerde gerçekleştirilecek işlemler de benzerdir.

Adımlar

SMTP Sunucusunun Kurulması

1. **Windows+R**'ye basın. **Run** iletişim kutusu görüntülenir.
2. **Open** metin kutusunda, `servermanager` girin ve **OK**'e tıklayın. **Server Manager** penceresi görüntülenir.
3. **Add Roles and Features** üzerine tıklayın. **Add Roles and Features Wizard** penceresi görüntülenir.
4. **Role-based or feature-based installation** seçimini yapın.
5. **Next** üzerine tıklayın.
6. **Select a server from the server pool** seçimini yapın ve ardından **Server Pool** içerisinden sunucuyu seçin.
7. **Add Roles and Features Wizard** içerisindeki **Features** adımı görüntülenene kadar **Next** üzerine tıklayın.
8. **SMTP Server**'ı seçin.
9. **Install** üzerine tıklayın.

IP Adresi ve Port Numarasının Yapılandırılması

10. **Control Panel > System and Security > Administrative Tools** içerisinde, **Internet Information Services (IIS) 6.0 Manager** üzerine çift tıklayın.
11. **SMTP Virtual Server #1** üzerine sağ tıklayın ve kısayol menüsünden **Properties'i** seçin. **[SMTP Virtual Server #1] Properties** iletişim kutusu görüntülenir. 12. **IP address** listesinden ilgili IP adresini seçin.

Not

Seçilen IP adresi, Adım 6'da seçilen sunucunun IP adresidir.

13. **Delivery** sekmesine geçin.
14. **Outbound connections** üzerine tıklayın. **Outbound Connections** iletişim kutusu görüntülenir. 15. **TCP port** metin kutusu içerisine `25` girin.
16. **OK** üzerine tıklayın.

4.12 Trap Notification Parametrelerinin Yapılandırılması.

Özet

Trap notification parametreleri, BMC tarafından alarmları tuzaklar (trap) aracılığıyla bir üçüncü taraf NMS'ine raporlamak için kullanılır.

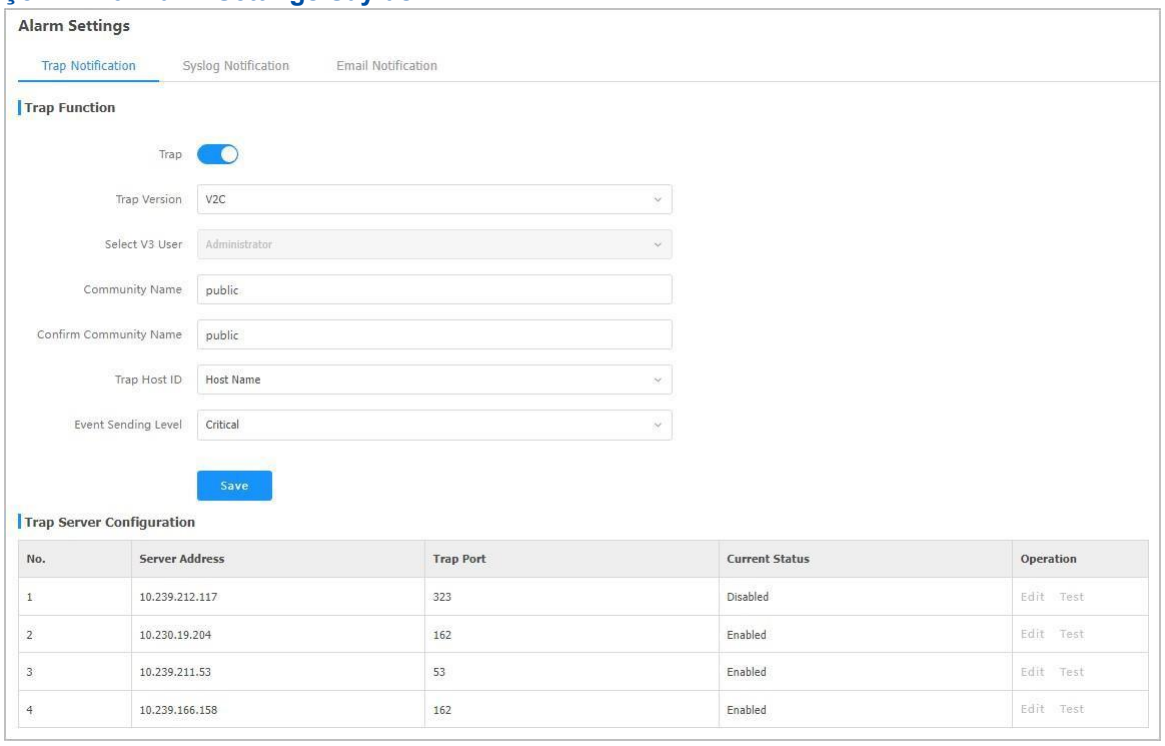
Not

Trap notification parametreleri, üçüncü taraf NMS'i tarafından sağlanır, dolayısıyla BMC'nin Web portalında ayarlanan trap notification parametrelerinin değerleri, üçüncü taraf NMS'indeki parametrelerin değerleriyle aynı olmalıdır.

Özet

1. **Maintenance'ı** seçin. **Maintenance** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Alarm Settings** seçimini yapın. **Alarm Settings** sayfası görüntülenir, bakınız Şekil 4-16.

Şekil 4-16 Alarm Settings Sayfası



3. **Trap Function** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 4-7'ye başvurun.

Tablo 4-7 Trap Function Parametre Açıklamaları

Parametre	Ayarlar
Trap	**Trap** anahtarını açın.
Trap Version	Tuzaklar için SNMP sürümünü seçin. Seçenekler: **V1**, **V2C** ve **V3**.
Select V3 User	**Trap Version** değeri **V3** olarak ayarlandıysa bu parametre gereklidir. SNMP üzerinden alarmları göndermek için izni olan bir kullanıcıyı seçin.
Community Name	**Trap Version** değeri **V1** veya **V2C** olarak ayarlandıysa bu parametre gereklidir. Tuzak topluluk adını girin.

Confirm Community Name	**Trap Version** değeri **V1** veya **V2C** olarak ayarlandıysa bu parametre gereklidir. Tuzak topluluk adını girin.
Trap Host ID	Alarmları raporlayan hostun tanımlayıcısını seçin.
Event Sending Level	Raporlanacak olayların seviyesini seçin. Örneğin, eğer **Event Sending Level** seviyesi **Critical** olarak ayarlandıysa sadece kritik alarmlar raporlanır.

4. **Save** üzerine tıklayın.
5. **Trap Server Configuration** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 4-8'e başvurun.

Tablo 4-8 Trap Server Configuration için Parametrelerin Açıklamaları

Parametre	Ayarlar
Server Address	Siz **Edit**'e tıkladıktan sonra parametre etkinleştirilir. Alarmları alan sunucunun adresini girin. Bir IPv4 adresi, IPv6 adresi veya domain adı desteklenir.
Trap Port	Siz **Edit**'e tıkladıktan sonra parametre etkinleştirilir. Alarmları alan sunucunun port numarasını girin. Aralık: 1–65535.
Current Status	Siz **Edit**'e tıkladıktan sonra parametre etkinleştirilir. Geçerli sunucuyu alarmları alması için etkinleştirip etkinleştirmeyeceğinizi seçin.

6. **Save** üzerine tıklayın.

Not

Edit butonu tıklandıktan sonra **Save** butonu olarak değişir.

7. (Opsiyonel) Sunucuya bir test olayı göndermek için **Test** üzerine tıklayın.

Not

Eğer sayfada "sent successfully" (başarıyla gönderildi) şeklinde bir ileti görüntülenirse, tuzak (trap) başarıyla gönderilmiştir.

4.13 BMC Loglarının Dışarı Aktarılması

BMC loglarını aşağıdaki yollarla dışarı aktarabilirsiniz:

- Logların Web portal üzerinden tek tıklamayla dışarı aktarılması

  Ayrıntılı bilgi için 4.13.1 Logların Web Portal Üzerinden Tek Tıklamayla Dışarı Aktarılması bölümüne başvurun.

- Logların Web Portal üzerinden kategoriye göre dışarı aktarılması

Ayrıntılı bilgi için 4.13.2 Logların Web Portal Üzerinden Kategoriye Göre Dışarı Aktarılması bölümüne başvurun.

- Logların SSH komutları üzerinden dışarı aktarılması

  Ayrıntılı bilgi için 4.13.3 Logların CLI (SSH) Üzerinden Dışarı Aktarılması bölümüne başvurun.

- Logların bir seri port üzerinden dışarı aktarılması

  Ayrıntılı bilgi için 4.13.4 Logların CLI (Seri Port) Üzerinden Dışarı Aktarılması bölümüne başvurun.

4.13.1 Logların Web Portal Üzerinden Tek Tıklamayla Dışarı Aktarılması

Özet

BMC'nin Web portalı, tek tıklamayla dışarı aktarma işlevi sağlar. Dışarı aktarılan log dosyasının adı *bmcinfo_<product serial number>.tar.gz* olup bu dosya tarayıcının varsayılan indirme dizininde saklanır.

Not

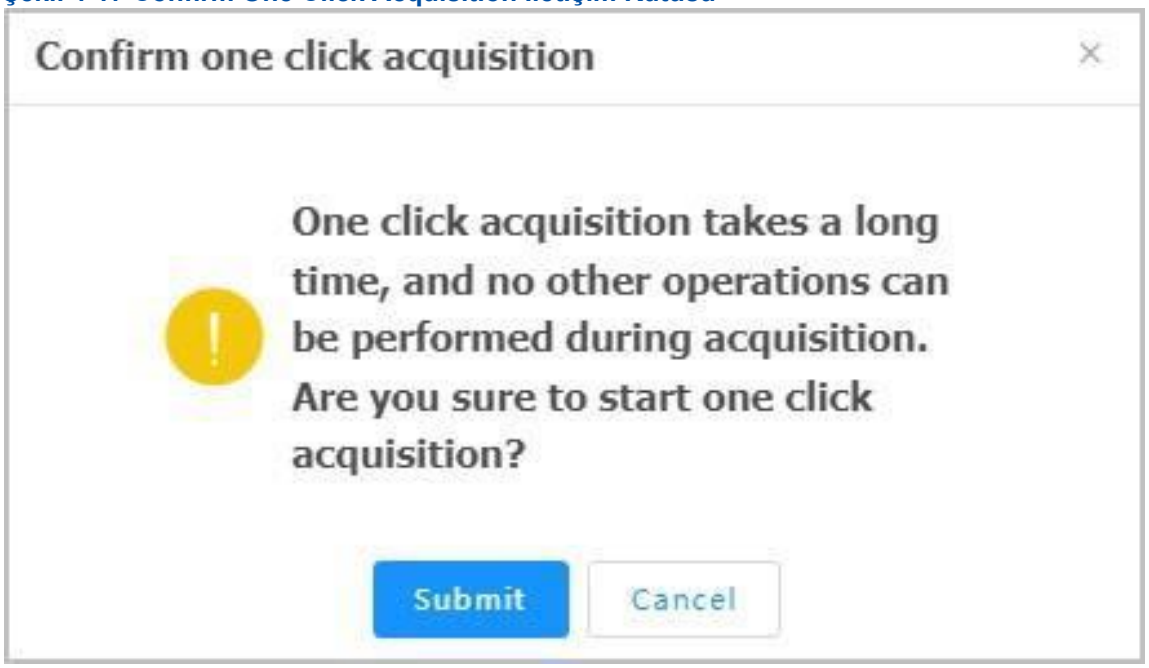
Eğer ürün seri numarası programlanmamışsa dosya adı şu şekildedir; *bmcinfo_UnknownProductSN.tar.gz*.

Adımlar

1. **Homepage** sayfasında **Shortcuts** alanında **One-Click Collection** üzerine tıklayın.

   Confirm one click acquisition iletişim kutusu görüntülenecektir, bakınız Şekil 4-17.

Şekil 4-17 Confirm One Click Acquisition İletişim Kutusu



2. **Submit** üzerine tıklayın.

Not

Toplama işlemi esnasında BMC'nin hiçbir Web arayüzü çalıştırılamaz.
Eğer tarayıcınızı yanlışlıkla kapatır ve BMC'nin Web portalında tekrar oturum açtıktan sonra logları toplarsanız, **One click acquisition is being processed, please try again later.** uyarı iletisi görüntülenir. Bu durumda, yaklaşık beş dakika beklemeniz gerekir.

4.13.2 Logların Web Portal Üzerinden Kategoriye Göre Dışarı Aktarılması

Özet

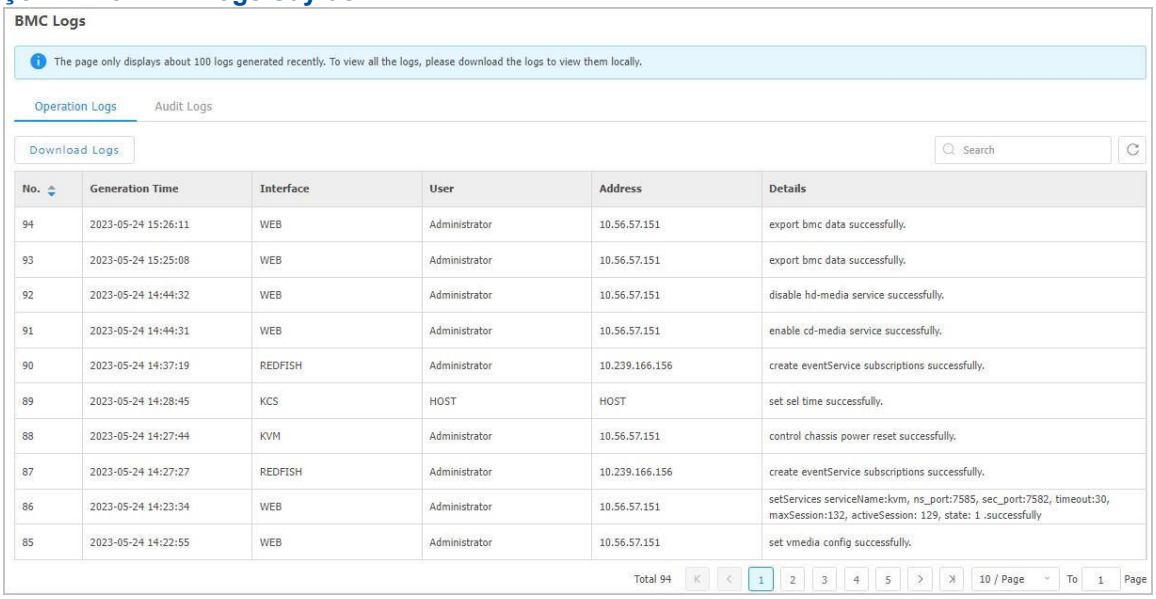
BMC'nin logları şunları içerir:

- **İşlem Logları (Operation Logs)**: kullanıcıların manuel olarak sunucu işlemleri ve uzaktan sunucu işlemleri gibi sunucu üzerinde yaptıkları işlemler hakkındaki bilgileri kaydeder.
- **Denetim Logları (Audit Logs)**: kullanıcıların Web portalı, BMC ve KVM'de oturum açma ve oturum kapatmalarını kaydeder.

Adımlar

1. **Maintenance'ı** seçin. **Maintenance** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **BMC Logs** seçimini yapın. **BMC Logs** sayfası görüntülenir, bakınız Şekil 4-18.

Şekil 4-18 BMC Logs Sayfası



3. Aşağıdaki işlemleri gerektiği gibi gerçekleştirin.

Aşağıdakileri gerçekleştirmek için...	**Şunları yapınız...**
İşlem loglarının dışarı aktarılması	a. **Operation Logs** sekmesine geçmek için **Operation Logs** üzerine tıklayın. b. (Opsiyonel) **Search** kutusu içerisine bir anahtar sözcük girin. c. **Download Logs** üzerine tıklayın.

Denetim loglarının dışarı aktarılması	a. **Audit Logs** sekmesine geçmek için **Audit Logs** üzerine tıklayın. b. (Opsiyonel) **Search** kutusu içerisine bir anahtar sözcük girin. c. **Download Logs** üzerine tıklayın.

4.13.3 Logların CLI (SSH) Üzerinden Dışarı Aktarılması

Özet

BMC'nin Web Portalı arızalandığında, BMC'ye SSH üzerinden oturum açabilir ve logları CLI üzerinden tek tıklamayla dışarı aktarabilirsiniz.

Adımlar

1. BMC'ye bir SSH aracı kullanarak bağlanın.
2. Logların dışarı aktarmak için CLI içerisinde aşağıdaki komutları çalıştırın:

```
# cd /etc/init.d/
# ./expert_data.sh
```

Not

Loglar dışarı aktarıldıktan sonra dizin içerisinde `/var/video/bmcinfo.tar.gz` .

3. SFTP işlevini kullanarak log dosyasını yerel PC'ye indirin.
4. BMC log dosyasını silmek için CLI içerisinde aşağıdaki komutları çalıştırın:

```
# cd /var/video
# rm bmcinfo.tar.gz
```

4.13.4 Logların CLI (Seri Port) Üzerinden Dışarı Aktarılması

Özet

Eğer bir ağ hatası nedeniyle BMC'ye erişilemiyorsa, logları seri port üzerinden tek tıklamayla dışarı aktarabilirsiniz.

Adımlar

1. Bir seri kablo kullanarak BMC'nin seri portuna bağlanın.
2. Sunucu panelindeki UID butonuna basın ve gösterge mavi renkte yanıp sönene kadar altı saniye boyunca basılı tutun.
3. Bir seri port aracı kullanarak BMC'nin seri portuna bağlanın.
4. Bağlantı kurulduktan sonra, ilgili kullanıcı adı ve parola ile seri portta oturum açın.
5. Logların dışarı aktarmak için CLI içerisinde aşağıdaki komutları çalıştırın:

```
# cd /etc/init.d/
# ./expert_data.sh
```

Not

Loglar dışarı aktarıldıktan sonra dizin içerisinde */var/video/bmcinfo.tar.gz* .

6. Log dosyasını */mnt/nandflash0/* dizinine yedeklemek için aşağıdaki komutu çalıştırın:

```
# cp /var/video/bmcinfo.tar.gz /mnt/nandflash0/
```

Not

Ağ geri yüklendikten sonra, SFTP işlevini kullanarak log dosyasını yerel PC'ye indirebilirsiniz.

4.14 BMC'nin Firmware'inin (Donanım Yazılımı) Yükseltilmesi

Özet

BMC'nin firmware'ının yükseltilmesi gerektiğinde, yükseltme işlemini gerçekleştirmek için firmware'ı çevrimiçi yükleyebilirsiniz.

Not

- BMC'nin firmware'ı yükseltildikten sonra BMC otomatik olarak sıfırlanır.
- Yükseltme işlemi sırasında bir firmware sürümü yükseltilemezse, bu firmware sürümünü yeniden yükseltmeniz gerekir.

Önkoşul

BMC'nin firmware'ı halihazırda alınmış olmalıdır.

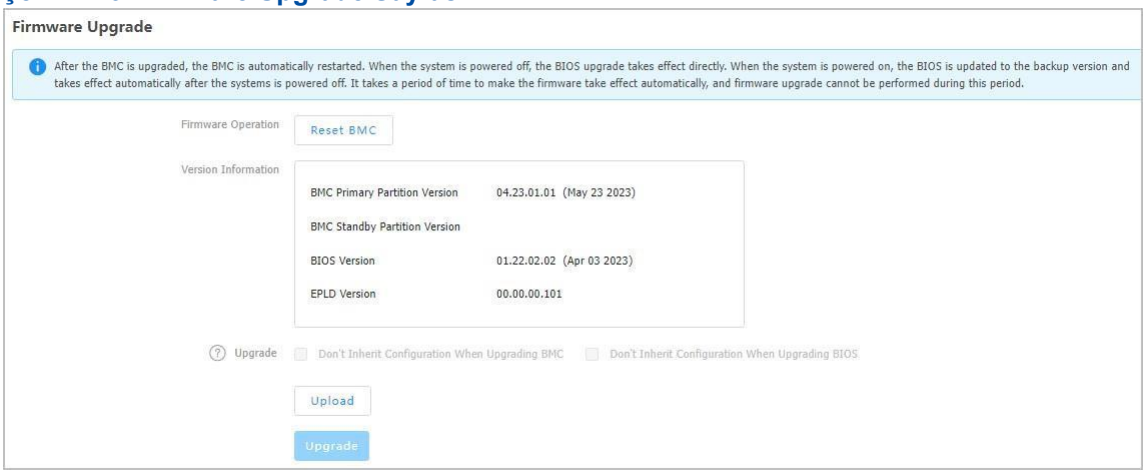
Not

Firmware yükseltme dosyası, sunucu ve depolama ürünlerinin Web portalındaki **Software Download** sayfasından indirilebilir (https://destek.netas.com.tr).

Adımlar

1. **BMC Settings'i** seçin. **BMC Settings** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Firmware Upgrade** seçimini yapın. **Firmware Upgrade** sayfası görüntülenir, bakınız Şekil 4-19.

Şekil 4-19 Firmware Upgrade Sayfası



3. **Upload** üzerine tıklayın ve firmware yükseltme dosyasını seçin.
4. **Upgrade** üzerine tıklayın.

Uyarı

Firmware yükseltme işlemi esnasında başka bir sayfaya geçemezsiniz. Aksi taktirde yükseltme işlemi kesintiye uğrar.

4.15 Varsayılan Fabrika Ayarlarını Geri Yükleme

Özet

Bu prosedürde sunucu yapılandırma öğelerinin (örneğin; ağ, kullanıcı, SNMP yapılandırması ve önyükleme modu) varsayılan fabrika ayarlarına nasıl döndürüleceği açıklanmıştır.

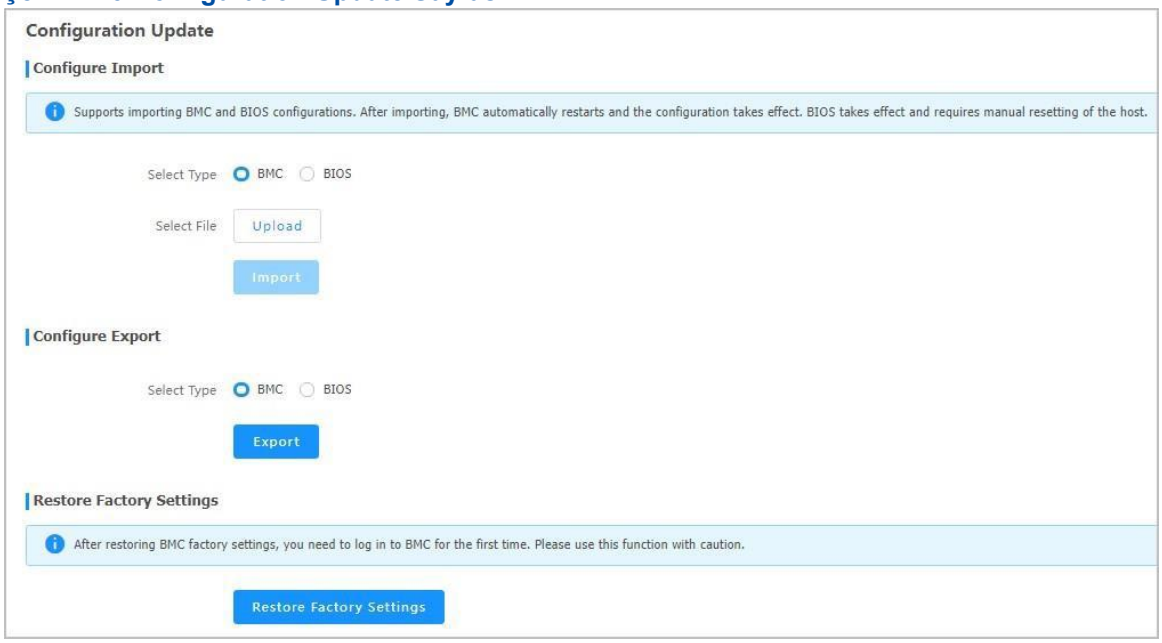
Not

Geri yükleme esnasında herhangi bir işlem gerçekleştirmeyin.
Varsayılan fabrika ayarları geri yüklendikten sonra, BMC otomatik olarak yeniden başlatılacaktır.

Adımlar

1. **BMC Settings'i** seçin. **BMC Settings** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Configuration Update** seçimini yapın. **Configuration Update** sayfası görüntülenecektir, bakınız Şekil 4-20.

Şekil 4-20 Configuration Update Sayfası



3. **Restore Factory Settings** üzerine tıklayın.

4.16 BMC Konfigürasyonlarının Yedeklenmesi

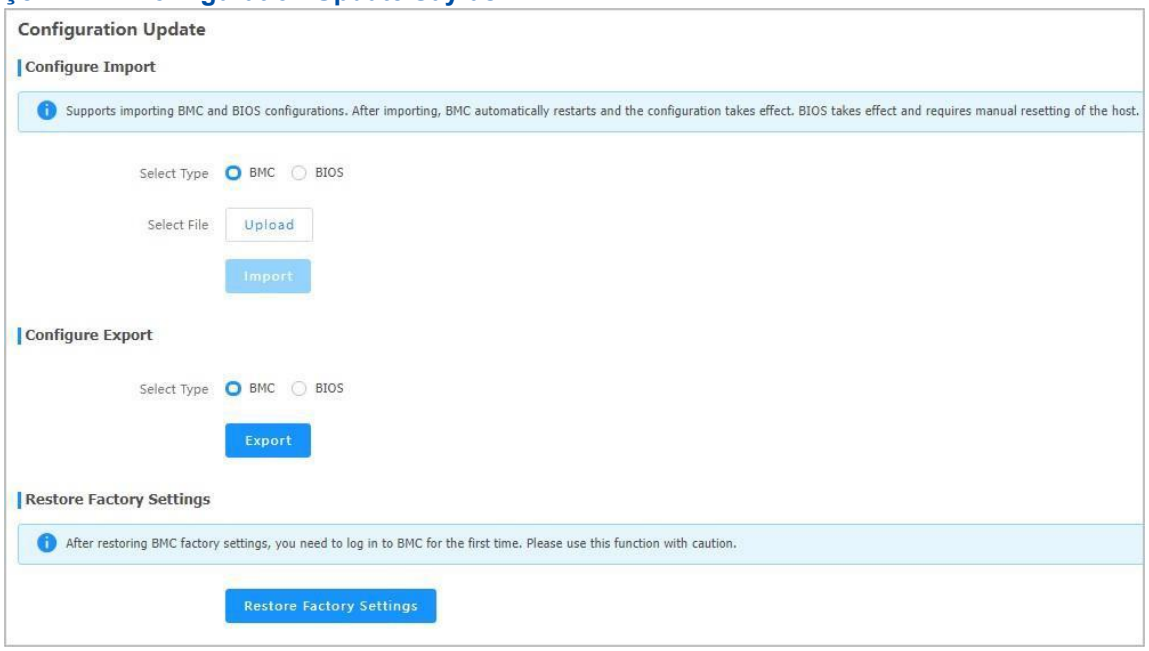
Özet

Sunucunun ana kartını değiştirmeden önce BMC konfigürasyonlarını dışarı aktarmanız gerekir. Ana kartı değiştirmeden önce, BMC konfigürasyonlarını içeri aktarmanız gerekir.

Adımlar

1. **BMC Settings'i** seçin. **BMC Settings** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Configuration Update** seçimini yapın. **Configuration Update** sayfası görüntülenecektir, bakınız Şekil 4-21.

Şekil 4-21 Configuration Update Sayfası



3. Geçerli BMC konfigürasyonlarını yerel PC'nize aktarmak için **Export** üzerine tıklayın.
4. Ana kartı değiştirdikten sonra **Upload** üzerine tıklayın ve görüntülenen iletişim kutusu içerisinde dışarı aktarılmış olan BMC konfigürasyonunu seçin.
5. **Import**'a tıklayın ve görüntülenen ileti kutusunda içeri aktarma işlemini onaylayın.

Not

BMC konfigürasyonları içeri aktarıldıktan sonra konfigürasyonların uygulanması için BMC otomatik olarak yeniden başlatılır. BMC yeniden başlatılana kadar hiçbir işlem gerçekleştirmeyin.

Bölüm 5
Sistem Yönetimi

İçindekiler Tablosu

5.1 Sistem Bilgilerinin Sorgulanması

Özet

Sistem bilgilerini sorgulayarak aşağıdaki bilgileri öğrenebilirsiniz:

- CPU bilgisi
- Bellek bilgisi
- Sabit disk bilgisi
- NIC ve FC bilgisi dahil NIC bilgisi
- FRU bilgisi
- Sensör bilgisi
- GPU ve PCIe kartı bilgileri dahil diğer bilgiler

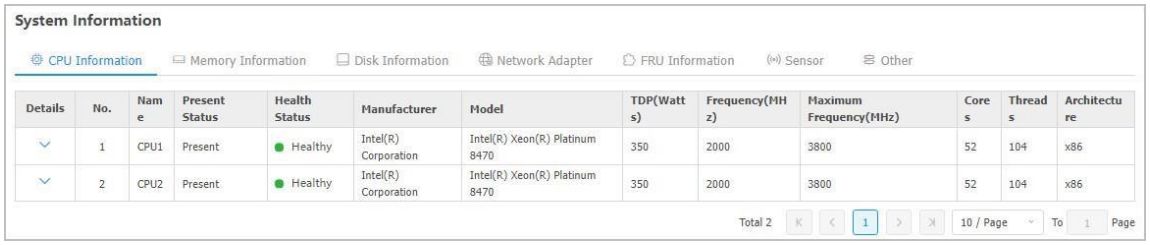
Not

Yukarıdaki bilgileri sorgulama işlemleri benzerdir. Bu prosedürde örnek olarak CPU bilgisinin nasıl sorgulanacağı verilmiştir.

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **System Information** seçimini yapın. **System Information** sayfası görüntülenir, bakınız Şekil 5-1.

Şekil 5-1 System Information Sayfası



3. (Opsiyonel) Bir CPU'nun ayrıntılarını görmek için, **Details** sütununda o CPU için  simgesine tıklayın

5.2 Performans Verilerinin Sorgulanması

Özet

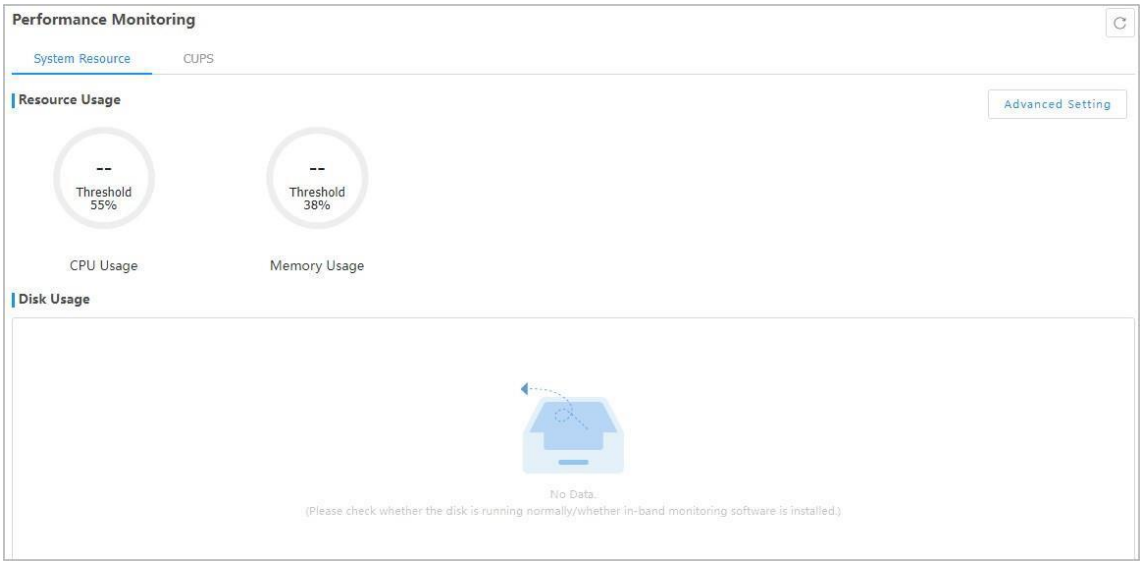
Performans verilerini sorgulayarak aşağıdaki bilgileri öğrenebilirsiniz:

- CPU kullanımı
- Bellek kullanımı
- Disk kullanımı
- Dinamik CPU yük oranı: mevcut durumda kullanılan CPU kaynaklarının sunucunun toplam CPU kaynaklarına oranıdır
- Dinamik bellek yük oranı: mevcut durumda kullanılan bellek kaynaklarının sunucunun toplam bellek kaynaklarına oranıdır
- Dinamik I/O yük oranı: mevcut durumda kullanılan I/O kaynaklarının sunucunun toplam I/O kaynaklarına oranıdır

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
4. Sol taraftaki navigasyon ağacından, **Performance Monitoring** seçimini yapın. **Performance Monitoring** sayfası görüntülenir, bakınız Şekil 5-2.

Şekil 5-2 Performance Monitoring Sayfası

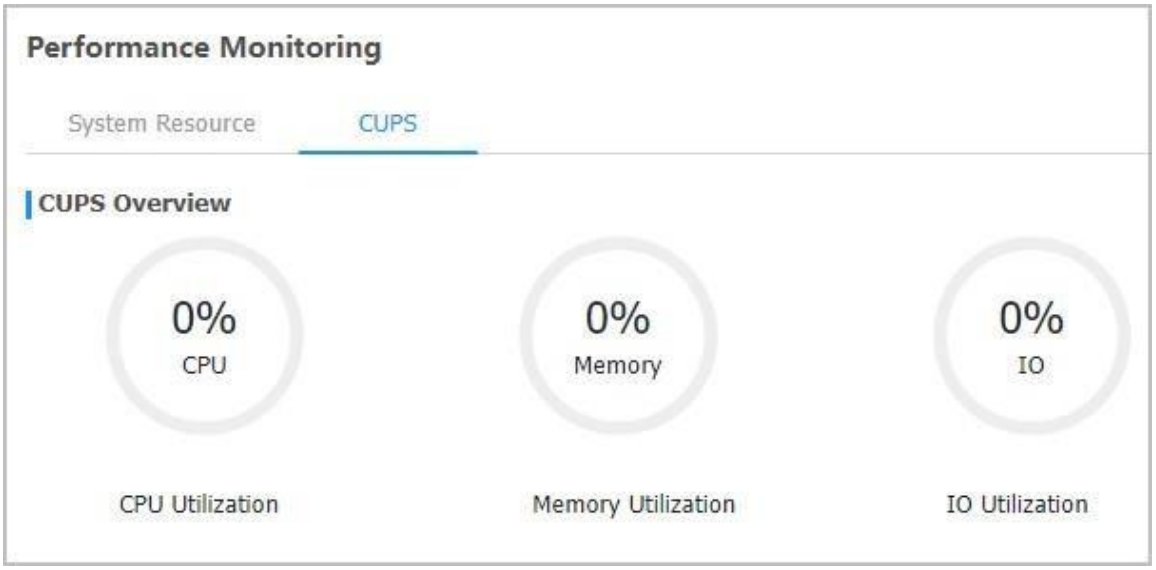


Not

Yukarıdaki sayfada, CPU kullanımı, bellek kullanımı ve disk kullanımı görüntülenir.

2. **CUPS** üzerine tıklayın. **CUPS** sekmesi görüntülenir, bakınız Şekil 5-3.

Şekil 5-3 CUPS Sekmesi



Not

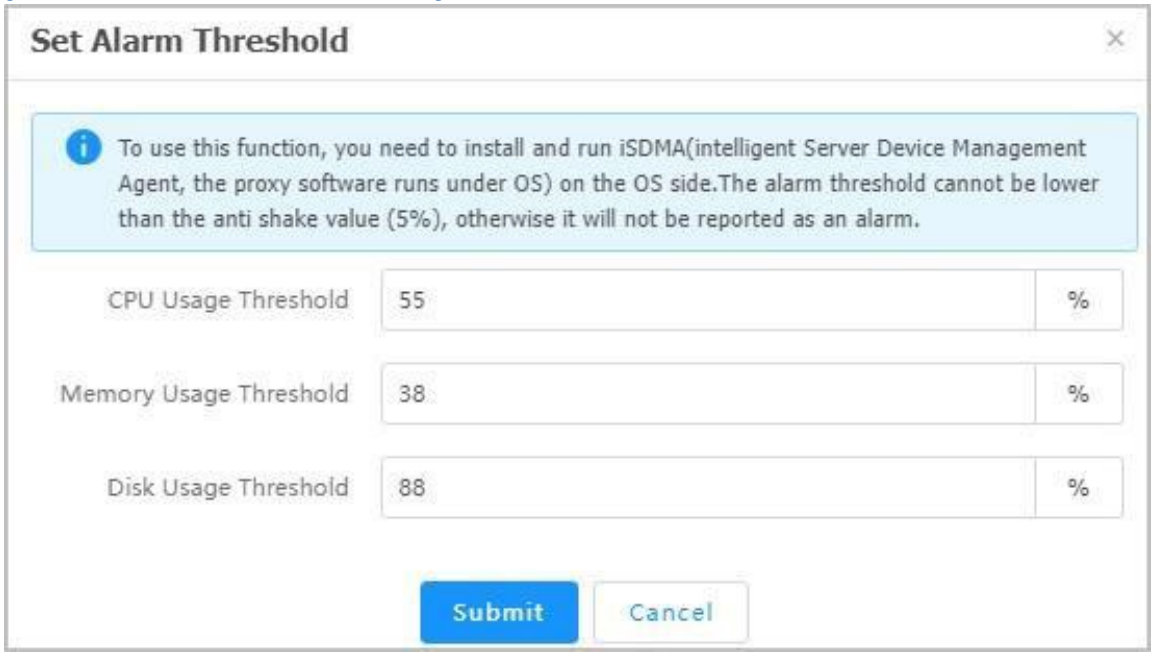
Yukarıdaki sekmede, Dinamik CPU, bellek ve I/O yük oranları görüntülenir.

İlgili Görevler

CPU kullanımı, bellek kullanımı ve disk kullanımı eşik değerlerini ayarlamak için aşağıdaki işlemleri gerçekleştirin:

1. **Performance Monitoring** sayfasında, **Advanced Setting** üzerine tıklayın. **Set Alarm Threshold** iletişim kutusu görüntülenir, bakınız Şekil 5-4.

Şekil 5-4 Set Alarm Threshold İletişim Kutusu



2. Alarm eşik değerini gerektiği gibi ayarlayın.
3. **Submit** üzerine tıklayın.

5.3 Fan Bilgisinin Sorgulanması

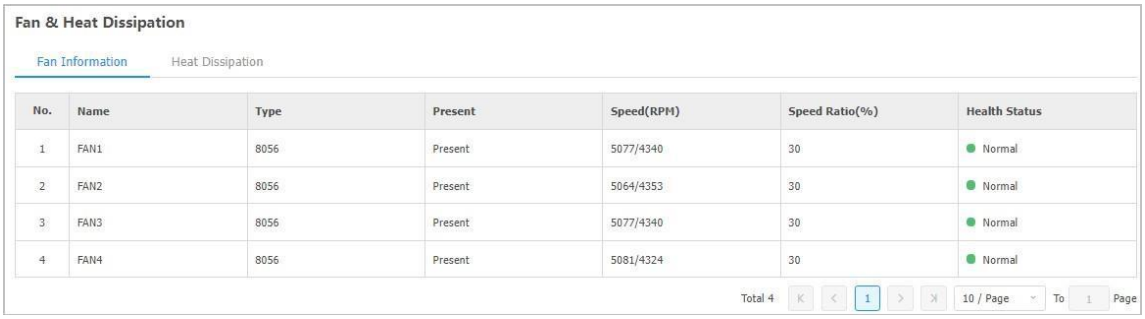
Özet

Fan bilgisini sorgulayarak, sunucudaki her bir fanın çalışma durumunu ve fan ile ilgili ayrıntılı bilgileri öğrenebilirsiniz.

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Fan & Heat Dissipation** seçimini yapın. **Fan & Heat Dissipation** sayfası görüntülenir, bakınız Şekil 5-5.

Şekil 5-5 Fan & Heat Dissipation Sayfası



Not

- **Speed(RPM)** sütunu, her bir fanın ön kanatlarının ve arka kanatlarının hızı dahil olmak üzere mevcut hızını belirtir. Örneğin, eğer **FAN1'**in hızı **5077/4340** ise ön kanatların hızı 5077 RPM ve arka kanatların hızı ise 4340 RPM'dir.
- **Speed Ratio(%)** sütunu,her bir fanın mevcut hızının maksimum hızına oranını belirtir.

5.4 Isı Yayılımı (Heat Dissipation) Politikasının Yapılandırılması.

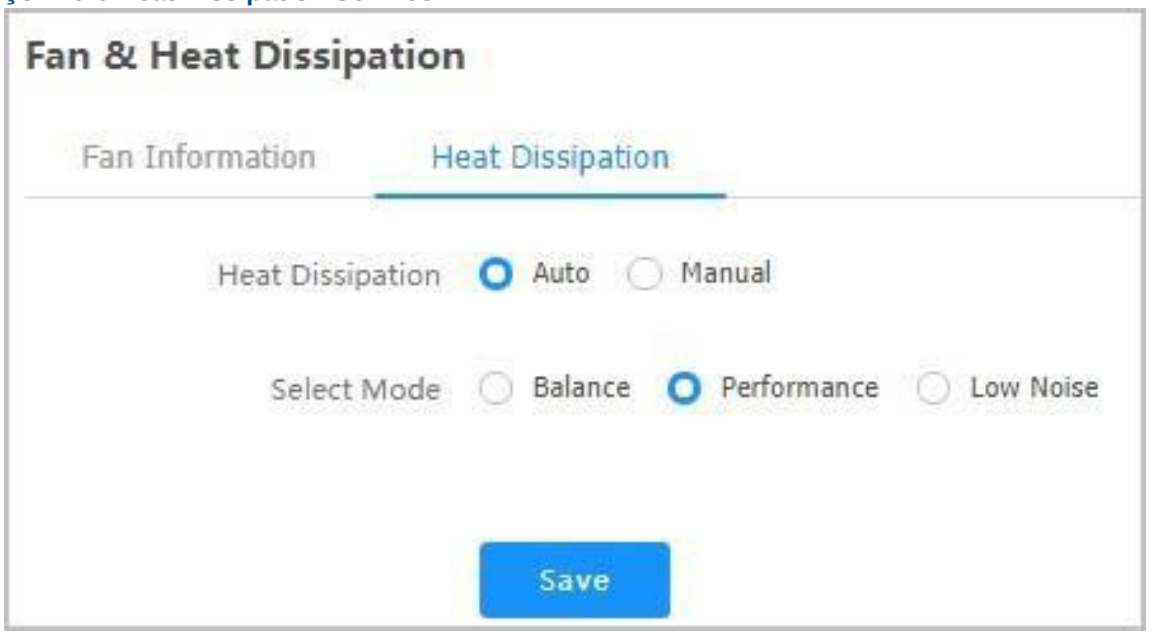
Özet

Isı yayılımı (heat dissipation) politikası, sunucunun performansını ve kararlılığını sağlamak için sunucunun bulunduğu ortama göre yapılandırılır.

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Fan & Heat Dissipation** seçimini yapın. **Fan & Heat Dissipation** sayfası görüntülenir.
3. **Heat Dissipation** üzerine tıklayın. **Heat Dissipation** sekmesi görüntülenir, bakınız Şekil 5-6.

Şekil 5-6 Heat Dissipation Sekmesi



4. Aşağıdaki işlemleri gerektiği gibi gerçekleştirin.

Eğer…	Yapmanız gereken işlem aşağıdaki gibidir...
Sunucunun üst yüzeyi üzerinde yer mevcutsa, ve sunucu gürültüye duyarlı değilse;	**Heat Dissipation'ı Auto** olarak ayarlayın ve ardından **Select Mode'yi Balance** olarak ayarlayın.
Eğer sunucular bir arada istiflenmişse, ve aralarında mesafe bırakılmamışsa,	**Heat Dissipation'ı Auto** olarak ayarlayın ve ardından **Select Mode'yi Performance** olarak ayarlayın.
Eğer sunucu bir ofiste veya gürültüye duyarlı başka bir alanda bulunuyorsa,	**Heat Dissipation'ı Auto** olarak ayarlayın ve ardından **Select Mode'yi Low Noise** olarak ayarlayın.
Fan hızının sunucu için manuel olarak ayarlanması gerekiyorsa,	**Heat Dissipation'ı Manual** olarak ayarlayın ve ardından **Speed Ratio** değerini ayarlayın .

Not

Speed Ratio, bir fanın mevcut hızının maksimum hızına oranını belirtir.

5. **Save** üzerine tıklayın.

5.5 Depolama Cihazlarının Yönetilmesi

Özet

Bir sunucunun depolama cihazları; RAID denetleyicilerini ve sabit diskleri ifade eder.

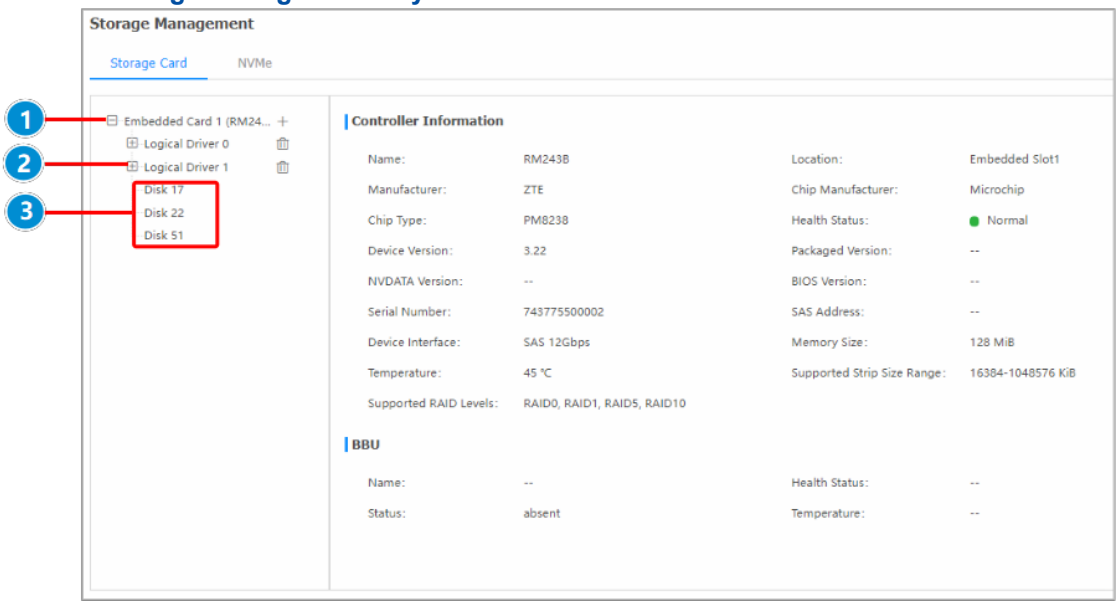
Bir RAID denetleyicisi tarafından yönetilen fiziksel diskler, mantıksal diskler olarak oluşturulabilir.

Sabit diskler arayüz türüne göre SAS diskleri ve NVMe diskleri olarak sınıflandırılabilirler. **Storage Management** sayfasındaki **Storage Card** sekmesi, SAS disklerini ve **NVMe** sekmesi de NVMe disklerini görüntüler.

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Storage Management** seçimini yapın. **Storage Management** sayfası görüntülenir, bakınız Şekil 5-7.

Şekil 5-7 Storage Management Sayfası



1. RAID denetleyici
2. Mantıksal disk
3. Fiziksel disk

3. Aşağıdaki işlemleri gerektiği gibi gerçekleştirin.

Aşağıdakileri gerçekleştirmek için...	**Şunları yapınız...**
RAID denetleyicisi ve BBU bilgilerinin kontrol edilmesi	**Storage Card** sekmesinde istediğiniz RAID denetleyicisine tıklayın. RAID denetleyicisi ve BBU bilgileri sağ tarafta görüntülenir.
Mantıksal disk bilgilerinin kontrol edilmesi	**Storage Card** sekmesinde istediğiniz mantıksal diske tıklayın. Detaylı mantıksal disk bilgisi sağ tarafta görüntülenir. Mantıksal disk bilgisinde **Status** aşağıdakileri içerir: • **Optimal** • **Degraded** • **Part Degraded** • **Offline**

Aşağıdakileri gerçekleştirmek için...	Şunları yapınız...
Bir mantıksal diskin UID göstergesinin ayarlanması.	a. **Storage Card** sekmesinde istediğiniz mantıksal diske tıklayın. b. Sağ taraftaki **Settings** üzerine tıklayın. **Logical Drive Setting** iletişim kutusu görüntülenir. c. **Open** ya da **Close** seçin. • **Open**: mantıksal diskin tüm üye disklerinin UID göstergelerini yakar. • **Off**: mantıksal diskin tüm üye disklerinin UID göstergelerini söndürür. d. **Submit** üzerine tıklayın.
Fiziksel disk bilgilerinin kontrol edilmesi	**Storage Card** sekmesinde istediğiniz fiziksel diske tıklayın. Detaylı fiziksel disk bilgisi sağ tarafta görüntülenir.
Bir mantıksal diskin oluşturulması	a. **Storage Card** sekmesinde RAID denetleyicisinin yanındaki **+** simgesine tıklayın. Sağ tarafta **Create Logical Drive** alanı görüntülenir, bakınız Şekil 5-8. b. Aşağıdaki parametreleri yapılandırın: • **Logical disk name**: Mantıksal diskin adını girin. • **RAID Level**: İlgili RAID seviyesini seçin. • **Stripe Size**: Bir stripe size değeri girin. • **Physical Drive Configuration**: Mantıksal diski oluşturan üye diskleri seçin. c. **Save** üzerine tıklayın.
NVMe disk bilgilerinin kontrol edilmesi	**Storage Management** sayfasında, **NVMe** sekmesine geçmek için **NVMe** üzerine tıklayın. Detaylı NVMe disk bilgisi görüntülenir.

Şekil 5-8 Create Logical Drive Alanı

Not

Mantıksal diskleri oluşturmak için farklı RAID denetleyici türlerinin farklı sayfaları vardır.

5.6 Sunucunun Açılması/Kapatılması

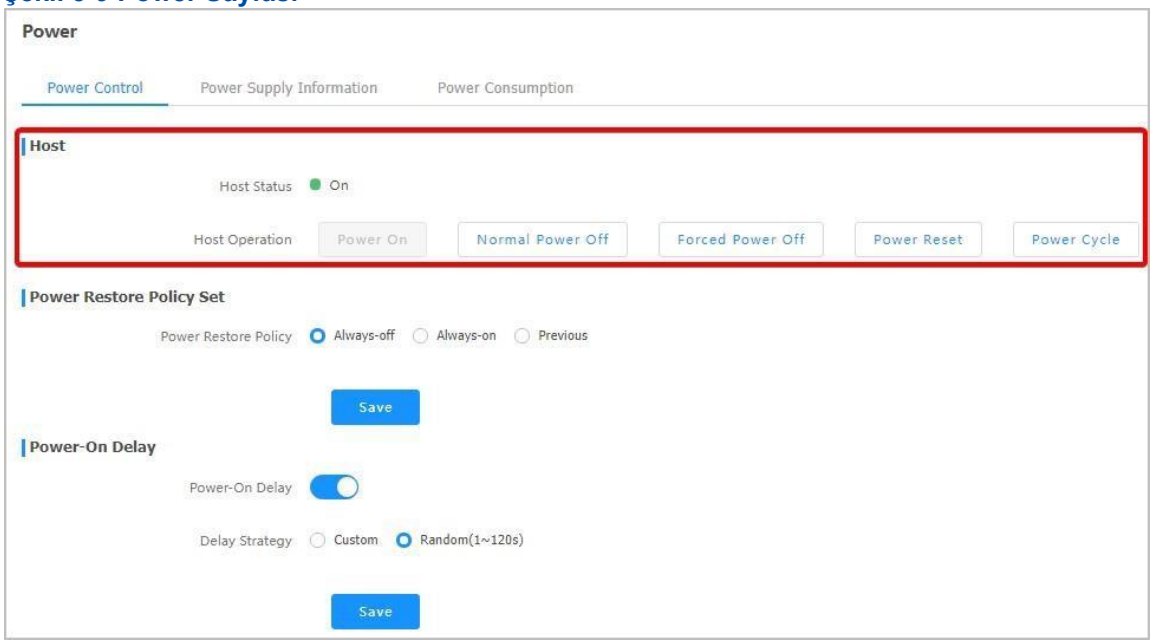
Özet

Müşteri sahasında bulunmadığınız zamanlarda sunucuyu açmak veya kapatmak için sunucuyu PC üzerinden uzaktan kontrol edebilirsiniz.

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Power** seçimini yapın. **Power** sayfası görüntülenir, bakınız Şekil 5-9.

Şekil 5-9 Power Sayfası



3. **Host** alanında **Host Status'ü** kontrol edin ve aşağıdaki işlemleri gerektiği biçimde gerçekleştirin:

Aşağıdakileri gerçekleştirmek için...	**Şunları yapınız...**
Sunucunun açılması	**Power On** üzerine tıklayın. Sunucu açılır.
Sunucunun kapatılması	**Normal Power Off** üzerine tıklayın. Sunucu kapatılır.
Sunucunun zorla kapatılması	**Forced Power Off** üzerine tıklayın. Sunucu zorla kapatılır.

Sunucu hemen yeniden başlatılması	**Power Reset** üzerine tıklayın. Sunucu kapatılır ve ardından açılır.
Aşağıdakileri gerçekleştirmek için...	**Şunları yapınız...**
Sunucunun zorla kapatılması ve ardından açılması	**Power Cycle** üzerine tıklayın. Sunucu zorla kapatılır ve ardından açılır.

Not

Gri renkli buton, sunucunun geçerli güç durumunu gösterir. Örneğin; **Power On** butonu gri renkli ise, sunucu güç açık durumundadır.

5.7 Sunucu Başlangıç (Startup) Politikasının Yapılandırılması

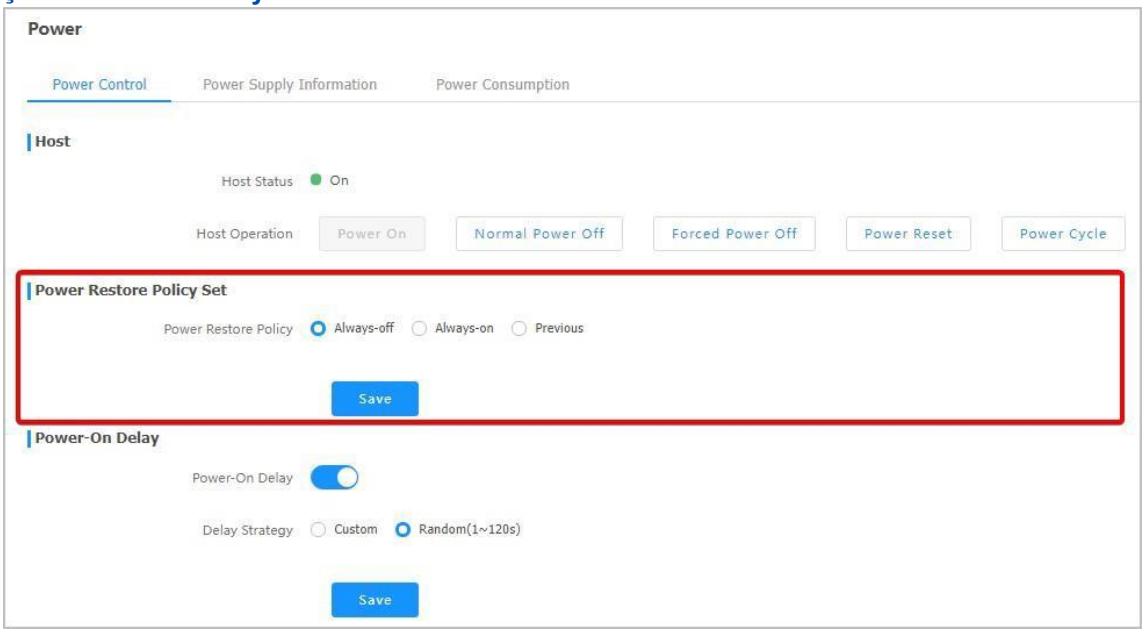
Özet

Bu prosedürde, güç geri yüklendikten sonra sunucunun güç durumunu belirlemek için sunucu başlatma politikasının nasıl yapılandırılacağını açıklamaktadır.

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Power** seçimini yapın. **Power** sayfası görüntülenir, bakınız Şekil 5-10.

Şekil 5-10 Power Sayfası



3. **Power Restore Policy Set** alanında, güç geri yüklendikten sonra sunucu başlangıç politikasını ayarlayın.
   - **Always-off**: Güç geri yüklendikten sonra sunucu kapalı kalır.
   - **Always-on**: Güç geri yüklendikten sonra sunucu otomatik olarak açılır.
   - **Previous**: Güç geri yüklendikten sonra sunucu önceki güç durumuna geri döner.
4. **Save** üzerine tıklayın.

5.8 Power-On Delay (Açılış Gecikmesi) Parametrelerinin Yapılandırılması

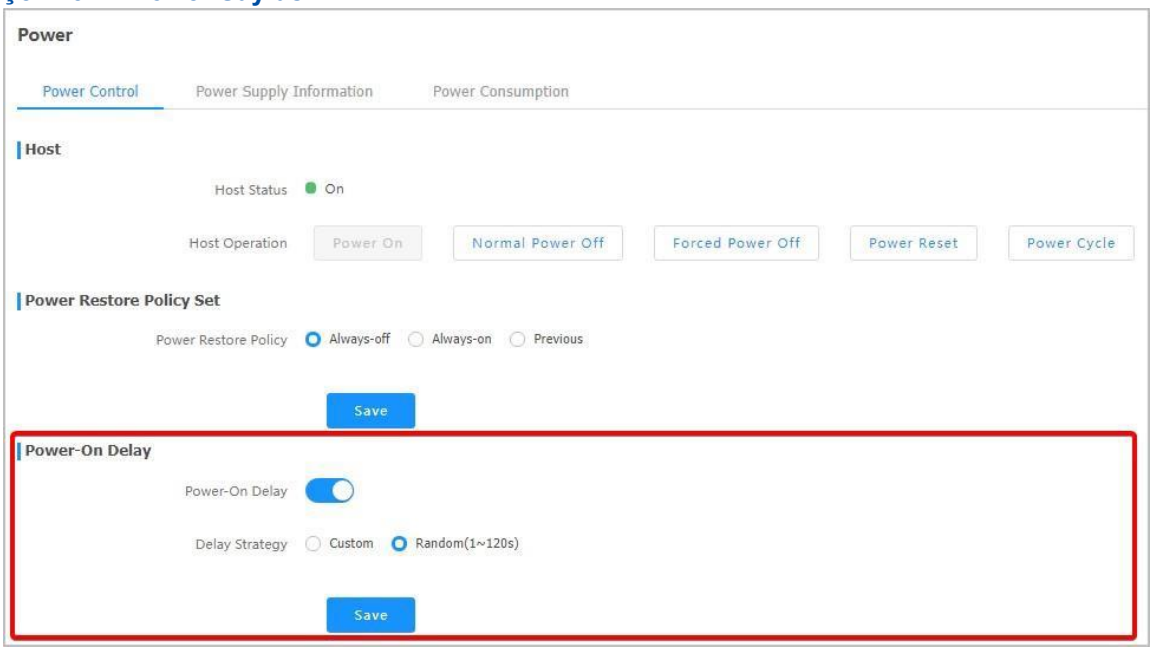
Özet

Bu prosedürde sunucuların açılışının kademeli hale getirilmesi için power-on delay (açılış gecikmesi) parametrelerinin nasıl ayarlanacağı açıklanmıştır.

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Power** seçimini yapın. **Power** sayfası görüntülenir, bakınız Şekil 5-11.

Şekil 5-11 Power Sayfası



3. **Power-On Delay** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 5-1'e başvurun.

Tablo 5-1 Power-On Delay Parametre Açıklamaları

Parametre	Ayarlar

Power-On Delay	Açılış gecikmesi işlevinin etkinleştirilip etkinleştirilmeyeceğini seçin. • Açılış gecikmesi işlevini etkinleştirmek için Power-On Delay anahtarını açın. • Açılış gecikmesi işlevini devre dışı bırakmak için Power-On Delay anahtarını kapatın.
Delay Strategy	İlgili açılış gecikmesi modunu seçin. • **Custom**: Açılış gecikmesi süresi kullanıcı tarafından tanımlanır.
Parametre	**Ayarlar**
	Eğer **Custom** seçilirse, **Custom Delay Duration** değerini ayarlayın. Aralık: 1–120, birim: saniye. • **Random**: Açılış gecikmesi süresi sistem tarafından otomatik olarak üretilir.

4. **Save** üzerine tıklayın.

5.9 Güç Kaynağı Bilgisinin Sorgulanması

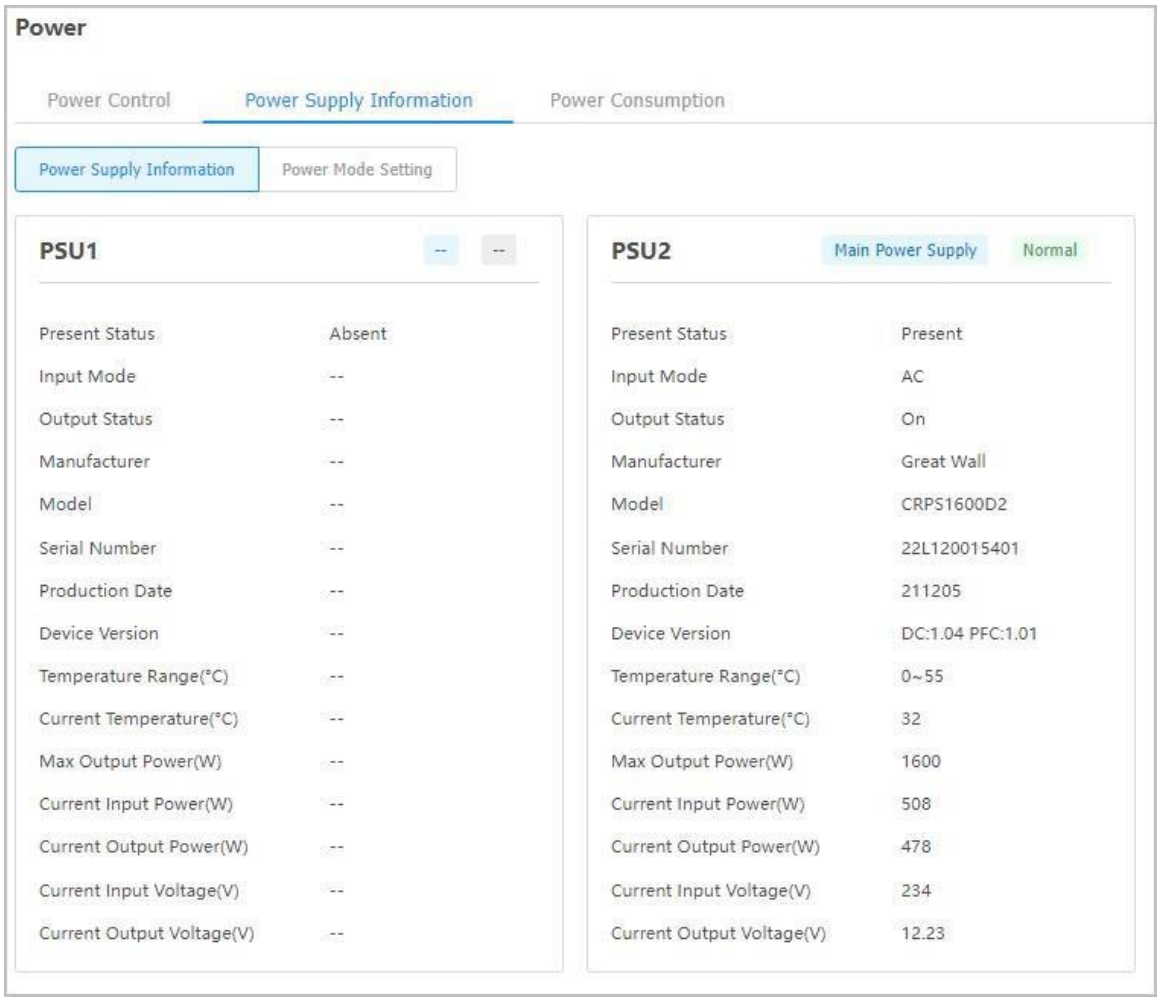
Özet

Güç kaynağı bilgisini sorgulayarak, sunucunun güç kaynakları hakkında bilgi edinebilirsiniz.

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Power** seçimini yapın. **Power** sayfası görüntülenir.
3. **Power Supply Information** üzerine tıklayın. **Power Supply Information** sekmesi görüntülenir, bakınız Şekil 5-12.

Şekil 5-12 Power Supply Information Sekmesi



Not

Güç kaynağı Input Mode aşağıdakileri içerir:

- AC
- HVDC
- LVDC

5.10 Power (Güç) Modunun Yapılandırılması

Özet

Sunucu güç modları aşağıdakileri içerir:

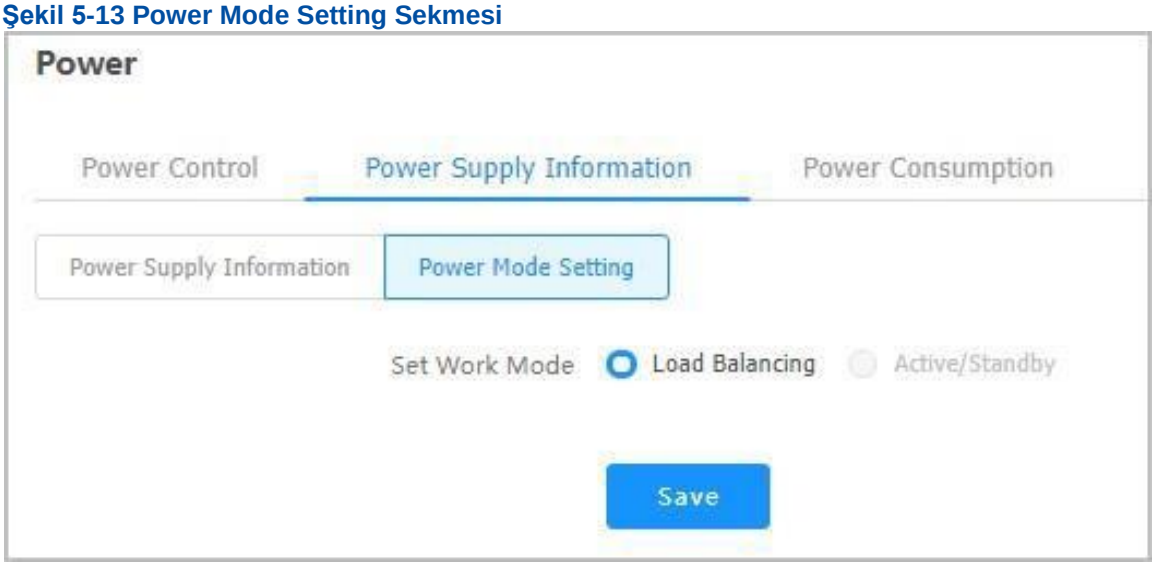
- **Load Balancing**: Güç modülleri, yük dengeleme modunda güç sağlar.
- **Active/Standby**: Güç modülleri, aktif/yedek modunda güç sağlar.

Güç modunun doğru olması güç modüllerinin sunucuya makul bir şekilde güç sağlayabilmesini mümkün kılar.

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Power** seçimini yapın. **Power** sayfası görüntülenir.
3. **Power Supply Information** üzerine tıklayın. **Power Supply Information** sekmesi görüntülenir.
4. **Power Mode Setting** üzerine tıklayın. **Power Mode Setting** sekmesi görüntülenir, bakınız Şekil 5-13.

Şekil 5-13 Power Mode Setting Sekmesi



5. Bir güç modu seçin.

Not

Active/Standby modu sadece iki adet veya daha fazla güç modülü mevcut ve **Normal** durumda olduğunda seçilebilir
.

6. **Save** üzerine tıklayın.

5.11 Güç İstatistiklerinin Sorgulanması

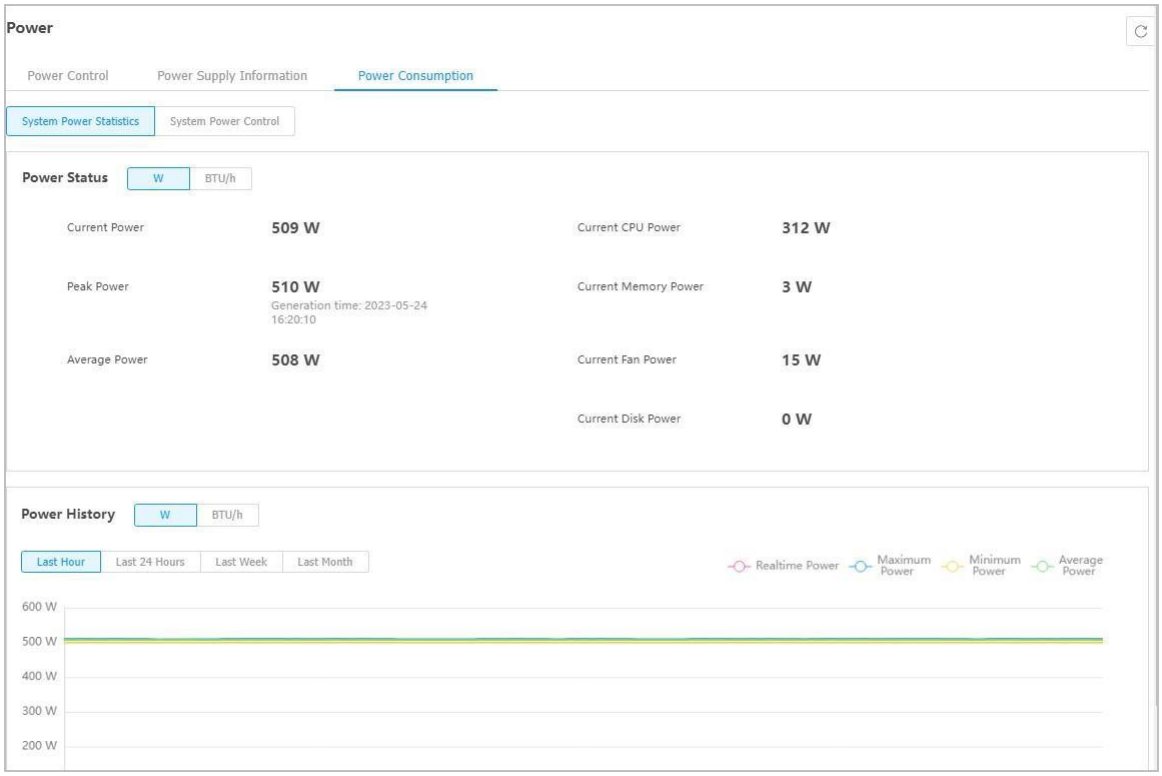
Özet

Güç istatistiklerini sorgulayarak, sunucunun mevcut güç durumunu ve belirlenen zaman aralığındaki güç değişikliklerini öğrenebilirsiniz.

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Power** seçimini yapın. **Power** sayfası görüntülenir.
3. **Power Consumption** üzerine tıklayın. **Power Consumption** sekmesi görüntülenir, bakınız Şekil 5-14.

Şekil 5-14 Power Consumption Sekmesi



Not

- Sunucunun geçerli güç istatistikleri, **Power Status** alanında görüntülenir.
- Sunucunun geçmiş güç istatistikleri, **Power History** alanında görüntülenir. İlgili güç istatistiklerini sorgulamak için bir zaman aralığı belirleyebilirsiniz.

5.12 Power Control (Güç Kontrolü) Parametrelerinin Yapılandırılması

Özet

Power Control parametreleri aşağıdakileri içerir:

- **Power Capping**: Sunucunun gücü, bir üst limit ile sınırlanır.
- **Power Threshold**: Sunucu gücü eşik değerini aştığında bir alarm verilir. Bu

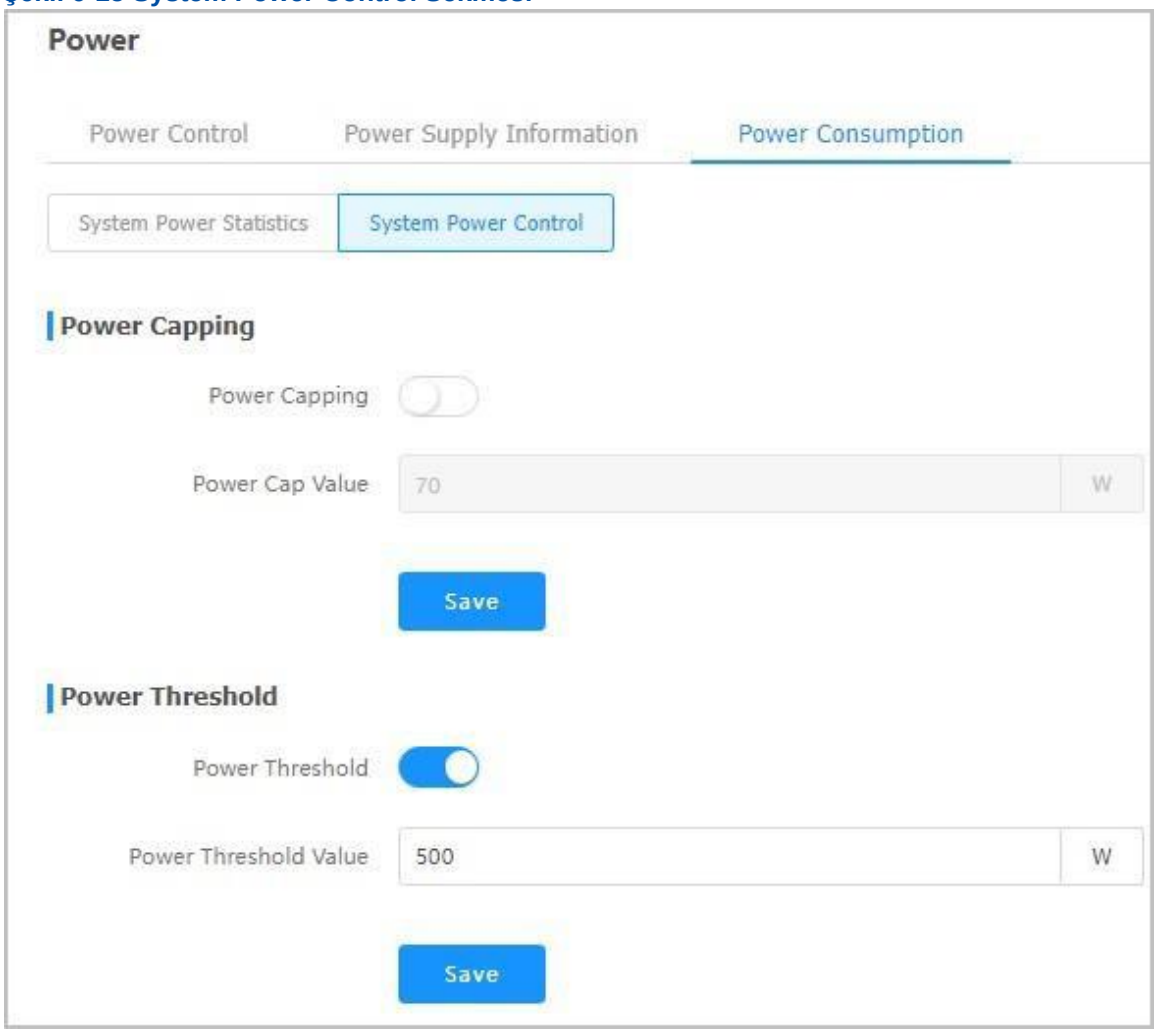
prosedürde güç kontrolü parametrelerinin nasıl yapılandırıldığı açıklanmıştır.

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Power** seçimini yapın. **Power** sayfası görüntülenir.
3. **Power Consumption** üzerine tıklayın. **Power Consumption** sekmesi görüntülenir.

4. **System Power Control** üzerine tıklayın. **System Power Control** sekmesi görüntülenir, bakınız Şekil 5-15.

Şekil 5-15 System Power Control Sekmesi



5. Aşağıdaki işlemleri gerektiği gibi gerçekleştirin.

Aşağıdakileri gerçekleştirmek için...	**Şunları yapınız...**
Güç üst limitinin ayarlanması	a. **Power Capping** alanında, **Power Capping** anahtarını açın. b. **Power Cap Value** metin kutusunda, güç üst limitini ayarlayın (aralık: 1– 32767, (birim: W). c. **Save** üzerine tıklayın.
Güç eşik değerinin ayarlanması	a. **Power Threshold** alanında, **Power Threshold** anahtarını açın. b. **Power Threshold Value** metin kutusunda, güç eşik değerini ayarlayın (aralık: 5– 32767, (birim: W). c. **Save** üzerine tıklayın.

5.13 Boot Options (Önyükleme Seçenekleri) Yapılandırılması

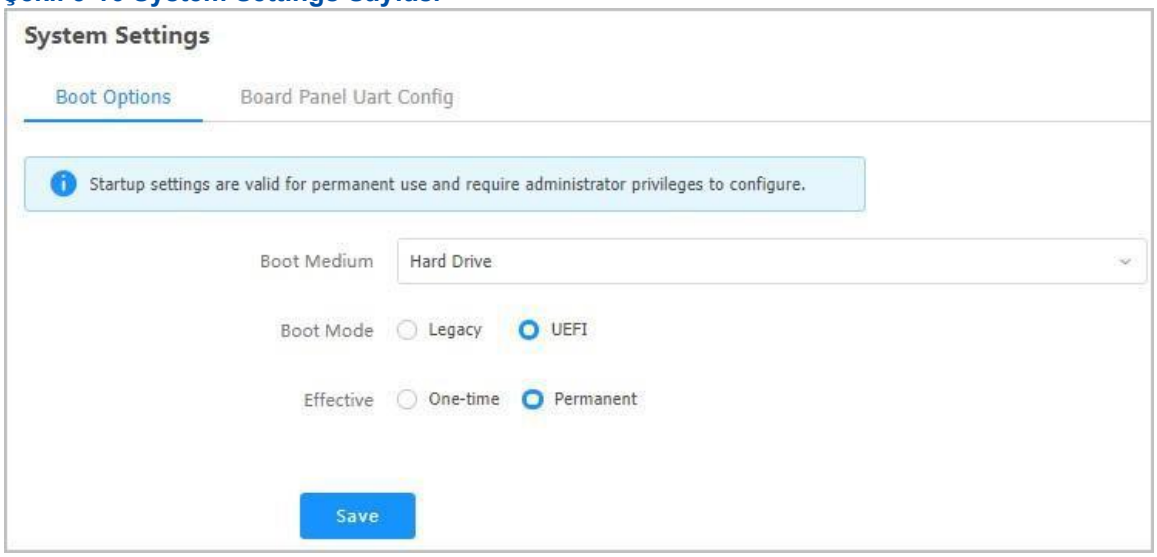
Özet

Bu prosedürde, sunucu için önyükleme cihazı, önyükleme modu ve önyükleme seçeneği verimliliğinin nasıl yapılandırılacağı açıklanmıştır.

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **System Settings** seçimini yapın. **System Settings** sayfası görüntülenir, bakınız Şekil 5-16.

Şekil 5-16 System Settings Sayfası



3. Parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 5-2'ye başvurun.

Tablo 5-2 Boot Option Parametre Açıklamaları

Parametre	Ayarlar
Boot Medium	Sunucuyu önyüklemek için kullanılan cihazı seçin. • **No Override**: hiçbir önyükleme cihazı yapılandırmaz ve BIOS'da yapılandırılmış olan varsayılan önyükleme cihazını kullanır. • **Hard Drive**:bir sabit diskten zorla önyükleme yapar. • **PXE**: PXE'den zorla önyükleme yapar. • **CD/DVD**: CD-ROM veya DVD-ROM sürücüsünden zorla önyükleme yapar. ● **BIOS Setup**: sunucu önyüklendikten sonra BIOS menüsüne girer. • **FDD/Removable Device**: bir disket sürücüsünden veya sökülüp takılabilen bir cihazdan (örneğin; USB) zorla önyükleme yapar.
Boot Mode	Bir sunucu önyükleme modu seçin. • **Legacy**: geleneksel bir önyükleme modu olup bazı sınırlamalara tabidir.

Parametre	Ayarlar
	• **UEFI**: daha yeni bir önyükleme modu olup bir IPv6/IPv4 ağında PXE işlevini destekler ve UEFI Shell ortamı sağlar. UEFI modu önerilir.
Effective	Yeniden yapılandırılan sunucu önyükleme seçeneklerinin sadece geçerli yeniden başlatma işlemine uygulanıp uygulanmayacağını seçin. • **One-time**: sadece geçerli yeniden başlatma işlemi için etkilidir. • **Permanent**: kalıcı olarak etkilidir.

4. **Save** üzerine tıklayın.

5.14 Seri Port Çıkışı Modunun Yapılandırılması

Özet

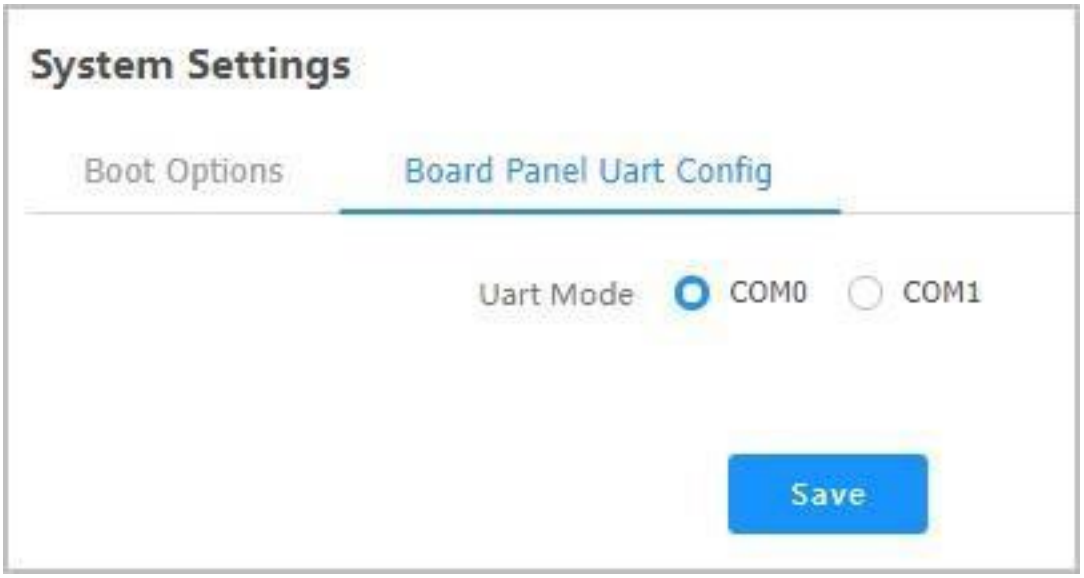
Panel üzerindeki seri port çıkışı modları aşağıdakileri içerir:

- COM1: Çıktı olarak BIOS fazında kaydedilen bilgiler sağlanır, bunlar BIOS'da yapılandırılabilir.
- COM2: BIOS fazında hiçbir çıktı yoktur ve sistem kısayol tuşu yanıt veremez. Çıktı olarak OS (İşletim Sistemi) fazında kaydedilen bilgiler sağlanır.

Adımlar

1. **System** seçin. **System** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **System Settings** seçimini yapın. **System Settings** sayfası görüntülenir.
3. **Board Panel Uart Config** üzerine tıklayın. **Board Panel Uart Config** sekmesi görüntülenir, bakınız Şekil 5-17.

4. **Şekil 5-17 Board Panel Uart Config Sekmesi**



5. Bir seri port çıkış modu seçin.
6. **Save** üzerine tıklayın.

Bölüm 6
Arıza Tespiti ve Bakım

İçindekiler Tablosu

6.1 Alarmların Sorgulanması

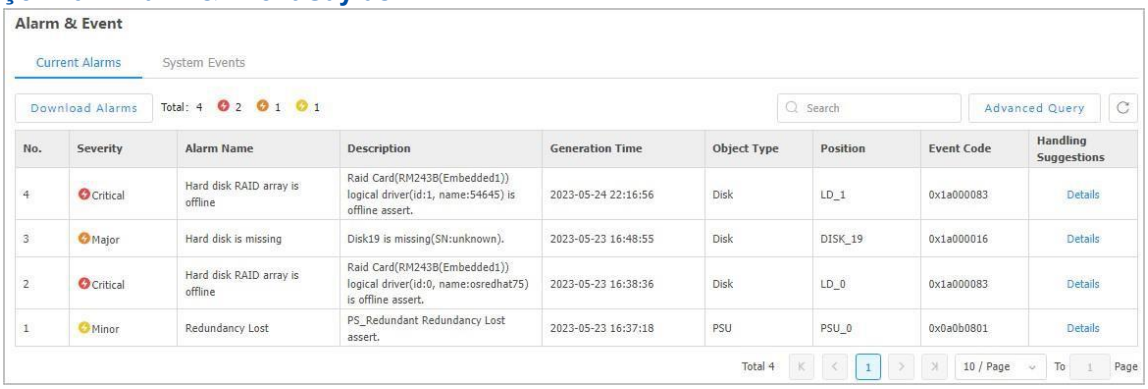
Özet

Alarmları sorgulayarak, sunucunun aktif alarmlarını ve sistem olaylarını öğrenebilirsiniz. Sistem olayları, bildirimleri ve temizlenen alarmları içerir.

Adımlar

1. **Maintenance'ı** seçin. **Maintenance** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Alarm & Event** seçimini yapın. **Alarm & Event** sayfası görüntülenir, bakınız Şekil 6-1.

Şekil 6-1 Alarm & Event Sayfası



3. Aşağıdaki işlemleri gerektiği gibi gerçekleştirin.

Aşağıdakileri gerçekleştirmek için...	**Şunları yapınız...**
Alarmları anahtar kelimeye göre sorgulamak	**Search** kutusu içerisine bir anahtar sözcük girin.
Alarmları gelişmiş parametrelere göre sorgulamak	a. **Advanced Query** üzerine tıklayın. Gelişmiş sorgulama koşulları görüntülenir. b. Sorgulama parametrelerini ayarlayın. c. **Query** üzerine tıklayın.
Bir alarmla başa çıkma önerilerini görüntüleyin	Alarm için **Details** üzerine tıklayın.
Alarm bilgilerini yerel bilgisayara kaydetmek	**Download Alarms** üzerine tıklayın.
Sistem olaylarını sorgulamak	**System Events** üzerine tıklayın. **System Events** sekmesi görüntülenir.

6.2 Alarm Raporlama Parametre Yapılandırması

Alarmlar aşağıdaki yollarla raporlanabilir:

- Tuzak (trap) paketleri aracılığıyla raporlama

  Tuzak bildirim parametrelerinin nasıl yapılandırılacağı hakkında bilgi almak için 6.2.1 Trap Notification Parametrelerinin Yapılandırılması bölümüne başvurun.

- Syslog paketleri aracılığıyla raporlama

  Syslog bildirim parametrelerinin nasıl yapılandırılacağı hakkında bilgi almak için 6.2.2 Syslog Notification Parametrelerinin Yapılandırılması bölümüne başvurun.

- E-posta yoluyla raporlama

  E-posta bildirim parametrelerinin nasıl yapılandırılacağı hakkında bilgi almak için 6.2.3 Email Notification Parametrelerinin Yapılandırılması bölümüne başvurun.

6.2.1 Trap Notification Parametrelerinin Yapılandırılması

Özet

Trap notification parametreleri, BMC tarafından alarmları tuzaklar (trap) aracılığıyla bir üçüncü taraf NMS'ine raporlamak için kullanılır.

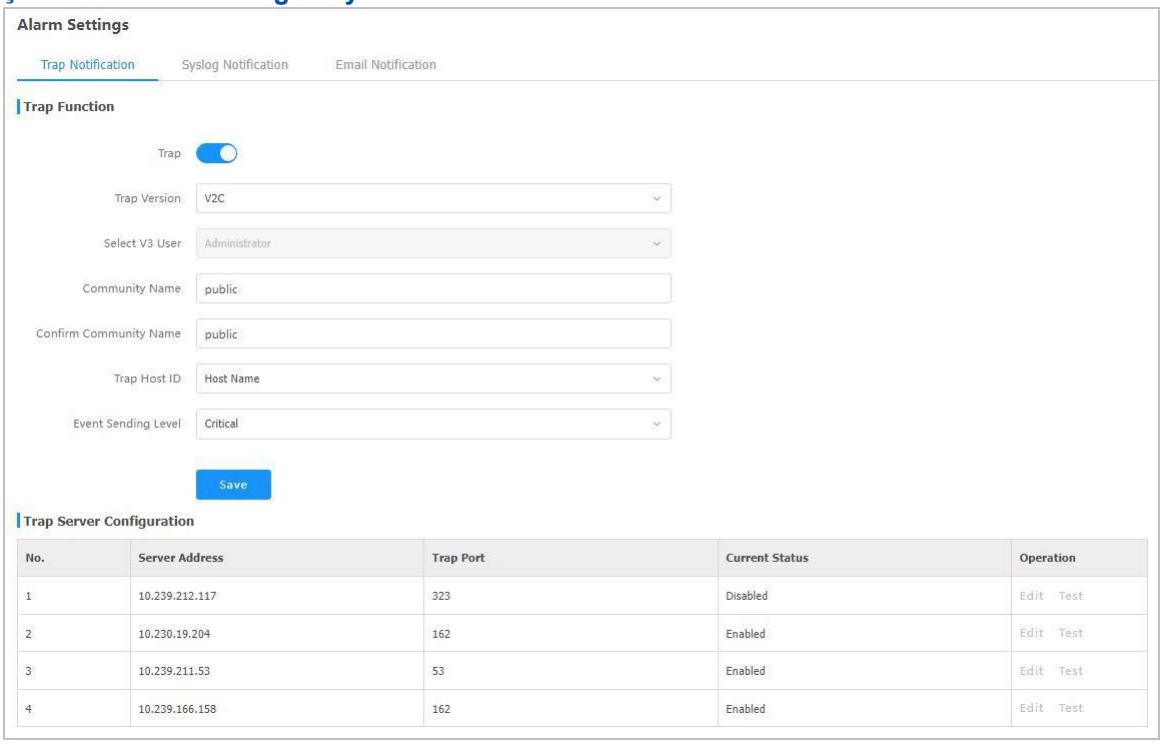
Not

Trap notification parametreleri, üçüncü taraf NMS'i tarafından sağlanır, dolayısıyla BMC'nin Web portalında ayarlanan trap notification parametrelerinin değerleri, üçüncü taraf NMS'indeki parametrelerin değerleriyle aynı olmalıdır.

Özet

1. **Maintenance'ı** seçin. **Maintenance** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Alarm Settings** seçimini yapın. **Alarm Settings** sayfası görüntülenir, bakınız Şekil 6-2.

Şekil 6-2 Alarm Settings Sayfası



Parametre	Ayarlar
Trap	**Trap** anahtarını açın.

Trap Version	Tuzaklar için SNMP sürümünü seçin. Seçenekler: **V1**, **V2C** ve **V3**.
Parametre	**Ayarlar**
Select V3 User	**Trap Version** değeri **V3** olarak ayarlandıysa bu parametre gereklidir. SNMP üzerinden alarmları göndermek için izni olan bir kullanıcıyı seçin.
Community Name	**Trap Version** değeri **V1** veya **V2C** olarak ayarlandıysa bu parametre gereklidir. Tuzak topluluk adını girin.
Confirm Community Name	**Trap Version** değeri **V1** veya **V2C** olarak ayarlandıysa bu parametre gereklidir. Tuzak topluluk adını girin.
Trap Host ID	Alarmları raporlayan hostun tanımlayıcısını seçin.
Event Sending Level	Raporlanacak olayların seviyesini seçin. Örneğin, eğer **Event Sending Level** seviyesi **Critical** olarak ayarlandıysa sadece kritik alarmlar raporlanır.

4. **Save** üzerine tıklayın.
5. **Trap Server Configuration** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 6-2'ye başvurun.

Tablo 6-2 Trap Server Configuration Parametrelerinin Açıklamaları

Parametre	**Ayarlar**
Server Address	Siz **Edit**'e tıkladıktan sonra parametre etkinleştirilir. Alarmları alan sunucunun adresini girin. Bir IPv4 adresi, IPv6 adresi veya domain adı desteklenir.
Trap Port	Siz **Edit**'e tıkladıktan sonra parametre etkinleştirilir. Alarmları alan sunucunun port numarasını girin. Aralık: 1–65535.
Current Status	Siz **Edit**'e tıkladıktan sonra parametre etkinleştirilir. Geçerli sunucuyu alarmları alması için etkinleştirip etkinleştirmeyeceğinizi seçin.

---

1. **Trap Function** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 6-1'e başvurun.

Tablo 6-1 Trap Function Parametre Açıklamaları

6. **Save** üzerine tıklayın.

Not

Edit butonu tıklandıktan sonra **Save** butonu olarak değişir.

7. (Opsiyonel) Sunucuya bir test olayı göndermek için **Test** üzerine tıklayın.

Not

Eğer sayfada "sent successfully" (başarıyla gönderildi) şeklinde bir ileti görüntülenirse, tuzak (trap) başarıyla gönderilmiştir.

6.2.2 Syslog Notification Parametrelerinin Yapılandırılması

Özet

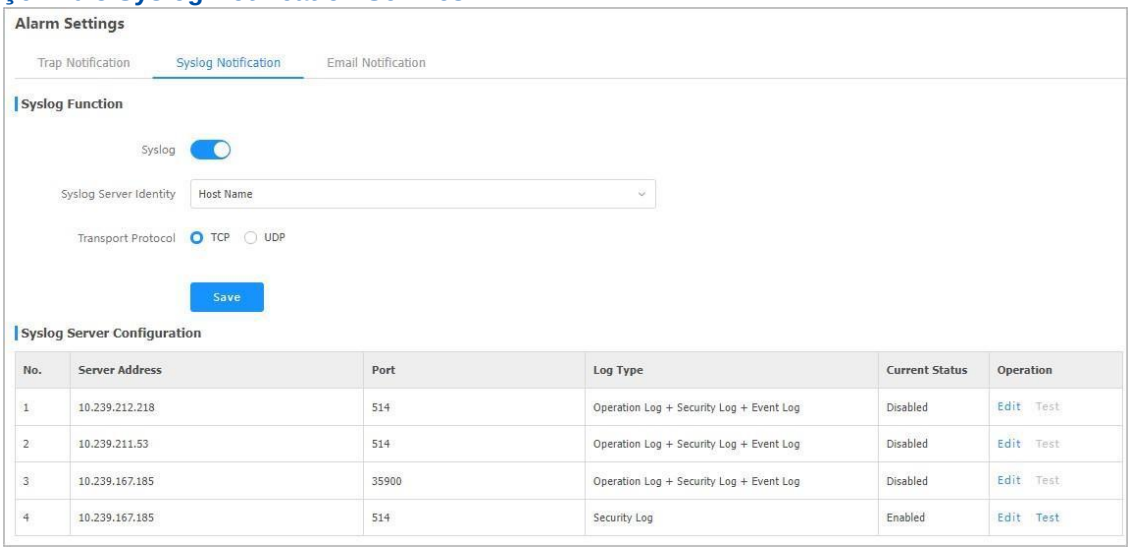
Bu prosedürde, BMC tarafından syslog sunucusuna log gönderilebilmesi için syslog bildirim parametrelerinin nasıl yapılandırıldığı açıklanmıştır. Gönderilen loglar aşağıdakileri içerir:

- **İşlem Logu (Operation Log)**: kullanıcıların manuel ve uzaktan gerçekleştirdikleri işlemler gibi donanım cihazları üzerinde yaptıkları işlemler hakkındaki bilgileri kaydeder.
- **Denetim Logu (Audit Log)**: kullanıcıların BMC'nin Web portalı, BMC ve KVM'de oturum açma ve oturum kapatmalarını kaydeder.
- **Event Log**: sunucunun çalıştırılması esnasında üretilen logları ve alarm bilgilerini kaydeder.

Özet

1. **Maintenance'ı** seçin. **Maintenance** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Alarm Settings** seçimini yapın. **Alarm Settings** sayfası görüntülenir.
3. **Syslog Notification** üzerine tıklayın. **Syslog Notification** sekmesi görüntülenir, bakınız Şekil 6-3.

Şekil 6-3 Syslog Notification Sekmesi



4. **Syslog Function** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 6-3'e başvurun.

Tablo 6-3 Syslog Function Parametre Açıklamaları

Parametre	Ayarlar
Syslog	**Syslog** anahtarını açın.
Syslog Server Identity	Logların gönderildiği syslog sunucusunun tanımlayıcısını seçin.
Transport Protocol	Bir log iletim protokolü seçin.

5. **Save** üzerine tıklayın.
6. **Syslog Server Configuration** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 6-4'e başvurun.

Tablo 6-4 Syslog Server Parametre Açıklamaları

Parametre	Ayarlar
Server Address	Siz **Edit**'e tıkladıktan sonra parametre etkinleştirilir. Syslog sunucusunun adresini girin. Bir IPv4 adresi, IPv6 adresi veya domain adı desteklenir.
Port	Siz **Edit**'e tıkladıktan sonra parametre etkinleştirilir. Syslog sunucusunun port numarasını girin. Aralık: 1–65535, varsayılan: 514.
Log Type	Siz **Edit**'e tıkladıktan sonra parametre etkinleştirilir. Bir veya daha fazla log türü seçin.
Current Status	Siz **Edit**'e tıkladıktan sonra parametre etkinleştirilir. Geçerli syslog sunucusunun logları alması için etkinleştirip etkinleştirmeyeceğinizi seçin.

7. **Save** üzerine tıklayın.

Not

Edit butonu tıklandıktan sonra **Save** butonu olarak değişir.

8. (Opsiyonel) Syslog sunucusuna bir test logu göndermek için **Test** üzerine tıklayın.

Not

Eğer sayfada "sent successfully" (başarıyla gönderildi) şeklinde bir ileti görüntülenirse,test logu başarıyla gönderilmiştir.

6.2.3 E-mail Notification Parametrelerinin Yapılandırılması

Özet

Bu prosedürde, BMC tarafından belirlenen posta kutusuna e-postalar gönderilebilmesi için e-posta bildirim parametrelerinin nasıl yapılandırıldığı açıklanmıştır.

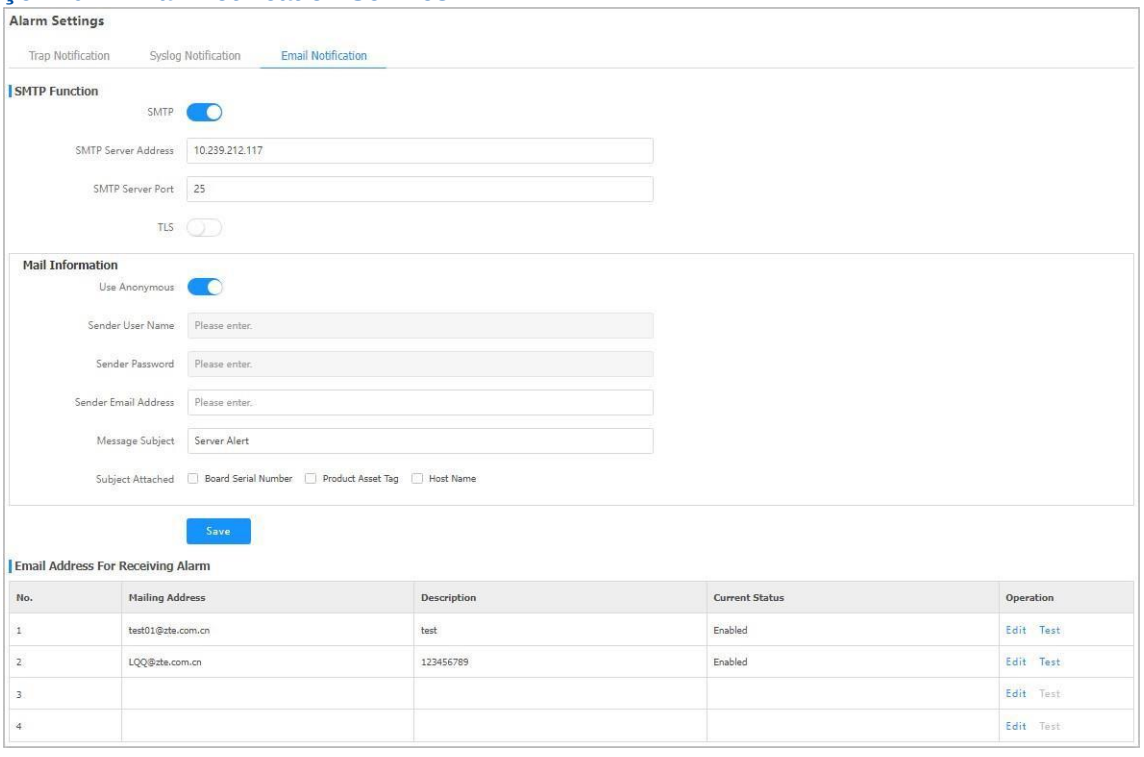
Önkoşul

Bir SMTP sunucusu halihazırda konuşlandırılmış olmalıdır. Detayları için 4.11 SMTP Sunucusunun Yapılandırılması bölümüne başvurun.

Özet

1. **Maintenance'ı** seçin. **Maintenance** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Alarm Settings** seçimini yapın. **Alarm Settings** sayfası görüntülenir.
3. **Email Notification** üzerine tıklayın. **Email Notification** sekmesi görüntülenir, bakınız Şekil 6-4.

Şekil 6-4 Email Notification Sekmesi



4. **SMTP Function** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 6-5'e başvurun.

Tablo 6-5 SMTP Function Parametre Açıklamaları

Parametre	Ayarlar

SMTP	**SMTP** anahtarını açın.
SMTP Server Address	SMTP sunucusunun IP adresini IPv4 veya IPv6 formatında girin.
SMTP Server Port	SMTP sunucusunun port numarasını girin. Aralık: 1–65535, varsayılan: 25.
TLS	Şifreleme işlevinin etkinleştirilip etkinleştirilmeyeceğini seçin.
Use Anonymous	E-postaların anonim olarak gönderilip gönderilmeyeceğini seçin.
Sender User Name	**Use Anonymous** anahtarı kapalı ise gereklidir. SMTP kimlik doğrulaması için kullanıcı adını girin.
Sender Password	**Use Anonymous** anahtarı kapalı ise gereklidir. E- posta göndericisinin parolasını girin.
Sender Email Address	Göndericinin e-posta adresini girin.
Parametre	**Ayarlar**
Message Subject	Alarm e-postalarının konusunu girin.
Subject Attached	E-postanın konusuna eklenecek bilgileri seçin. Bir veya daha fazla seçim yapılabilir.

5. **Save** üzerine tıklayın.
6. **Email Address For Receiving Alarm** alanında parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 6-6'ya başvurun.

Tablo 6-6 Mailbox Address Adres Parametre Açıklamaları

Parametre	**Ayarlar**
Mailing Address	Siz **Edit**'e tıkladıktan sonra parametre etkinleştirilir. Alarmların gönderildiği e-posta adresini girin.
Description	Siz **Edit**'e tıkladıktan sonra parametre etkinleştirilir. E-posta adresinin açıklamasını girin.
Current Status	Siz **Edit**'e tıkladıktan sonra parametre etkinleştirilir. Geçerli e-posta adresini alarmları alması için etkinleştirip etkinleştirmeyeceğinizi seçin.

7. **Save** üzerine tıklayın.

Not

Edit butonu tıklandıktan sonra **Save** butonu olarak değişir.

8. (Opsiyonel) E-posta adresine bir test alarm e-postası göndermek için **Test** üzerine tıklayın.

Not

Eğer sayfada "sent successfully” (başarıyla gönderildi) şeklinde bir ileti görüntülenirse,alarm e-postası başarıyla gönderilmiştir.

6.3 Bir Ekran Görüntüsünün Alınması

Özet

Ekran görüntüsü işlevi, arıza tespiti için kullanılır.

Not

Ekran görüntüsü alma işlevini kullanmadan önce, KVM işlevini devre dışı bırakmanız gerekir.

Ekran görüntüsü aşağıdaki yollarla alınabilir:

- Otomatik

  Aşağıdaki koşullardan birisi tetiklendiğinde otomatik olarak ekran görüntüsü alınır:

  → Onarılamaz bir hata (fatal error) (örneğin; bir CPU arızası) meydana geldikten sonra sunucu yeniden başlatılır.

  → BMC tarafından **Power Reset** işleminin tetiklenmesi.

  → BMC tarafından **Power Cycle** işleminin tetiklenmesi.

  → BMC tarafından **Forced Power Off** işleminin tetiklenmesi.

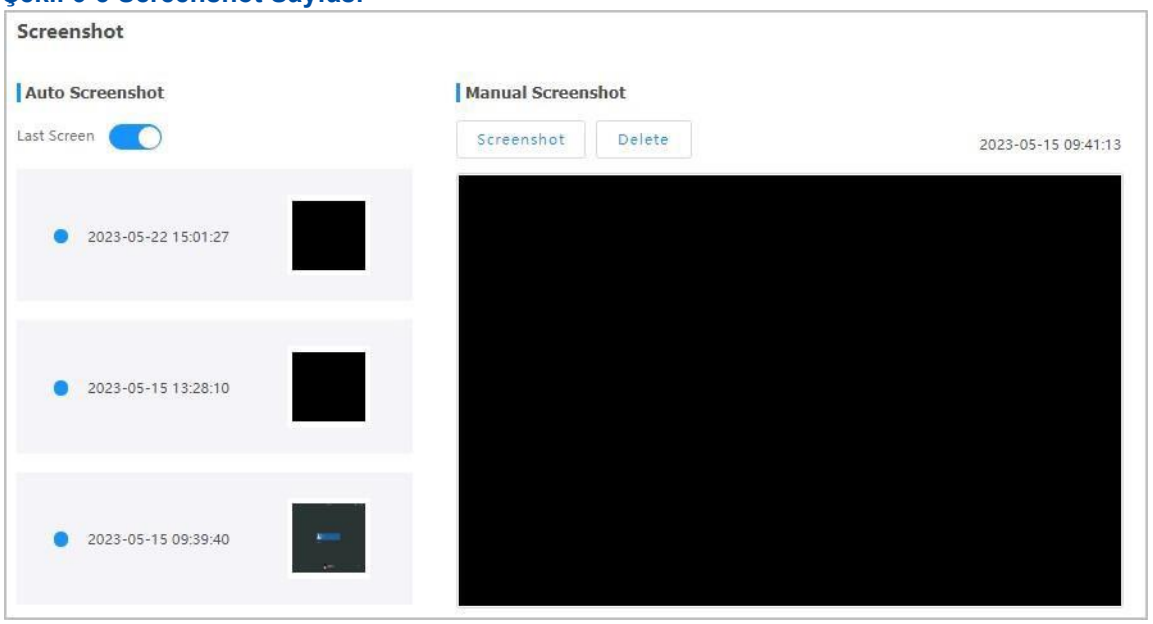
  BMC tarafından tetiklenebilen güç işlemlerinin açıklaması için 5.6 Sunucunun Açılması/Kapatılması bölümüne başvurun.

- Manuel olarak

Adımlar

1. **Maintenance'ı** seçin. **Maintenance** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Screenshot** seçimini yapın. **Screenshot** sayfası görüntülenir, bakınız Şekil 6-5.

Şekil 6-5 Screenshot Sayfası



3. Aşağıdaki işlemleri gerektiği gibi gerçekleştirin.

Aşağıdakileri gerçekleştirmek için...	Şunları yapınız...
Otomatik olarak ekran görüntüleri almak	**Last Screen** anahtarını açın.
Manuel olarak bir ekran görüntüsü almak	**Screenshot** üzerine tıklayın. Geçerli ekranın ekran görüntüsü sayfanın alt kısmında görüntülenir. Geçerli ekran görüntüsünü silmek için **Delete** üzerine tıklayın.

6.4 POST (Açılışta Otomatik Sınama) Kodlarının Görüntülenmesi

Özet

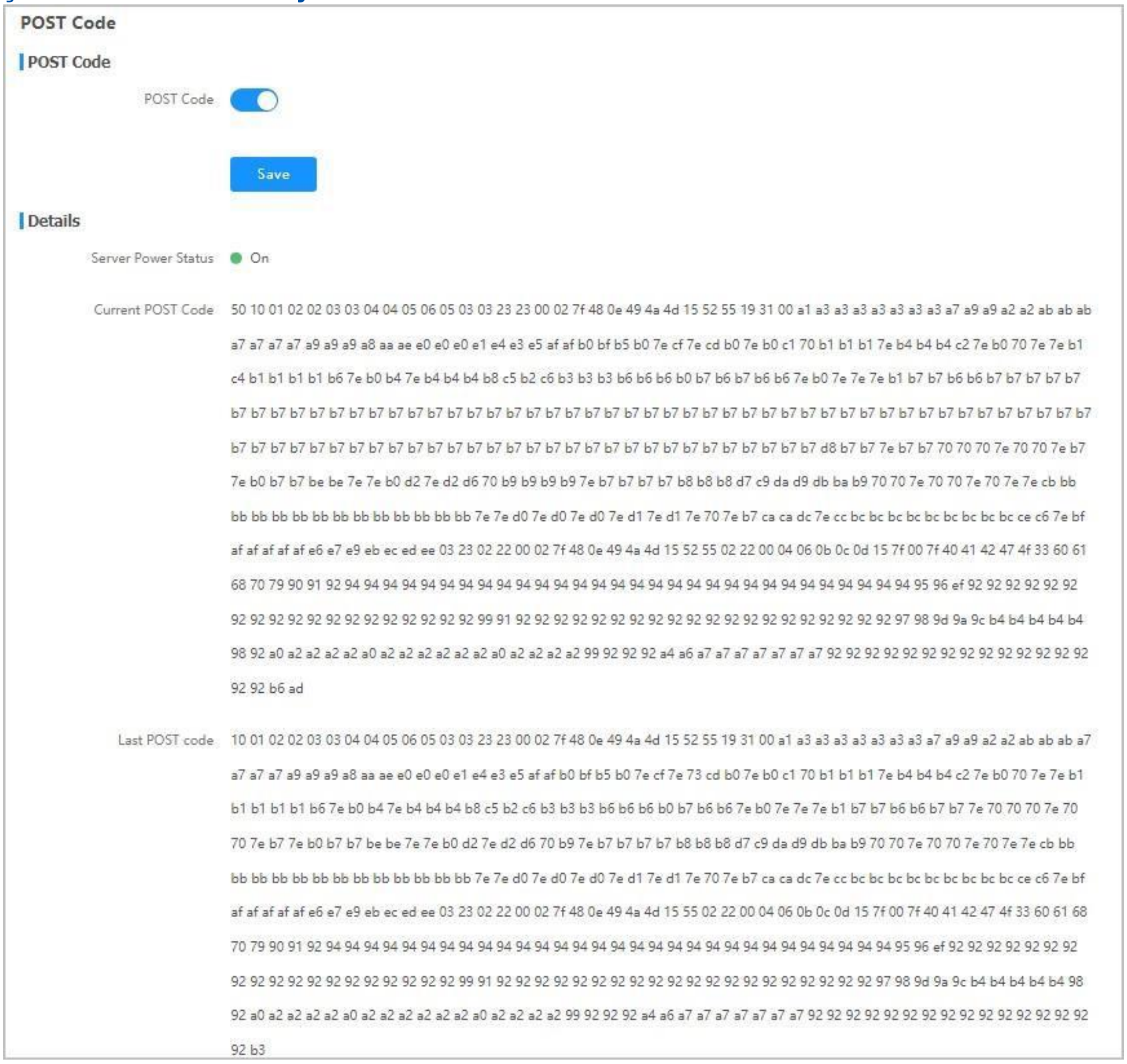
POST kodu, sunucunun açılışı esnasındaki durumunu kaydeder.

Arıza tespiti için POST kodunu kontrol edin.

Adımlar

1. **Maintenance'ı** seçin. **Maintenance** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **POST Code** seçimini yapın. **POST Code** sayfası görüntülenir, bakınız Şekil 6-6.

Şekil 6-6 POST Code Sayfası



3. (Opsiyonel) Eğer POST kodu etkinleştirilmemiş ise, **POST Code'u** açın ve **Save** üzerine tıklayın.
4. **Server Power Status**, **Current POST Code** ve **Last POST Code** bilgilerini görüntüleyin.

6.5 Sunucu Loglarının İndirilmesi

Özet

Bir arıza meydana geldiğinde, sunucu logları, seri porta yazılır. Arıza tespiti için bu logları indirebilirsiniz.

Adımlar

1. **Maintenance'ı** seçin. **Maintenance** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Host Logs** seçimini yapın. **Host Logs** sayfası görüntülenir, bakınız Şekil 6-7.

Şekil 6-7 Host Log Sayfası

3. **Download** üzerine tıklayın.

6.6 BMC Loglarının Sorgulanması

Özet

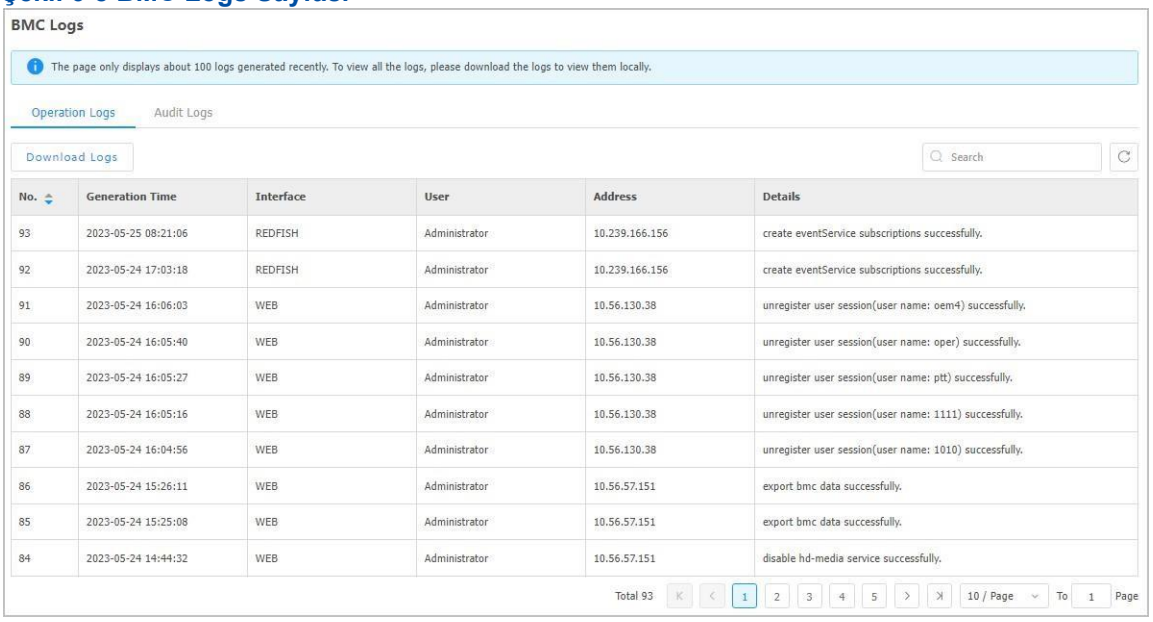
BMC loglarının aşağıdakileri içerir:

- **İşlem Logları (Operation Logs)**: kullanıcıların manuel olarak ve uzaktan gerçekleştirdikleri işlemler gibi sunucu üzerinde yaptıkları işlemler hakkındaki bilgileri kaydeder.
- **Denetim Logları (Audit Logs)**: kullanıcıların BMC'nin Web portalı, BMC ve KVM'de oturum açma ve oturum kapatmalarını kaydeder.

Adımlar

1. **Maintenance'ı** seçin. **Maintenance** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **BMC Logs** seçimini yapın. **BMC Logs** sayfası görüntülenir, bakınız Şekil 6-8.

Şekil 6-8 BMC Logs Sayfası



3. Aşağıdaki işlemleri gerektiği gibi gerçekleştirin.

Aşağıdakileri gerçekleştirmek için...	Şunları yapınız...

İşlem loglarını sorgulamak	a. **Operation Logs** sekmesine geçmek için **Operation Logs** üzerine tıklayın. b. (Opsiyonel) **Search** kutusu içerisine bir anahtar sözcük girin. c. (Opsiyonel) **Download Logs** üzerine tıklayın.
Denetim loglarını sorgulamak	a. **Audit Logs** sekmesine geçmek için **Audit Logs** üzerine tıklayın. b. (Opsiyonel) **Search** kutusu içerisine bir anahtar sözcük girin. c. (Opsiyonel) **Download Logs** üzerine tıklayın.

6.7 SEL Loglarının Sorgulanması

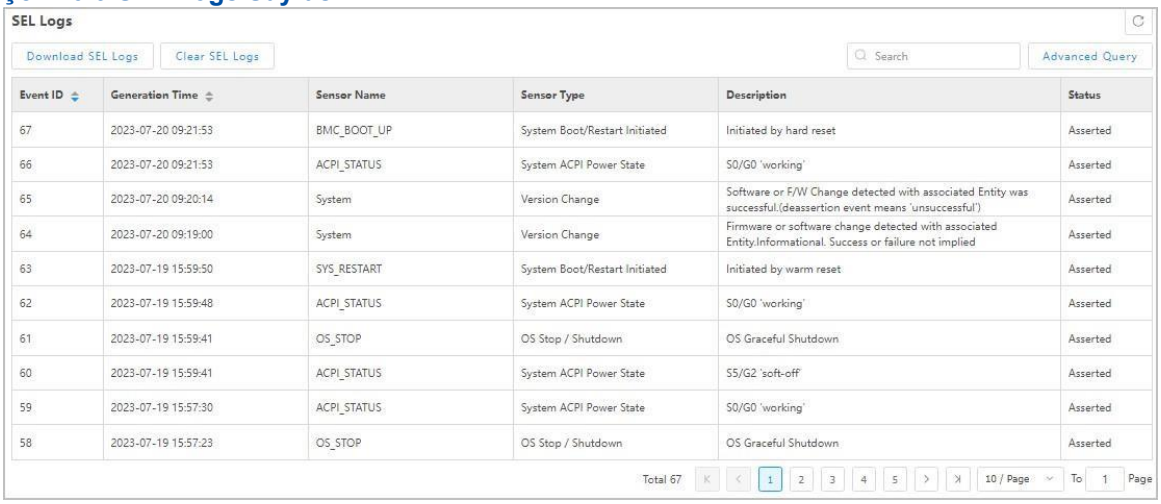
Özet

SEL logları, sunucu sistemindeki sensörler tarafından raporlanan olay loglarını kaydeder.

Adımlar

1. **Maintenance'ı** seçin. **Maintenance** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **SEL Logs** seçimini yapın. **SEL Logs** sayfası görüntülenir, bakınız Şekil 6-9.

Şekil 6-9 SEL Logs Sayfası



3. (Opsiyonel) **Advanced Query** üzerine tıklayın, sorgulama koşullarını ayarlayın ve **Query** üzerine tıklayın.
4. Aşağıdaki işlemleri gerektiği gibi gerçekleştirin.

Aşağıdakileri gerçekleştirmek için...	**Şunları yapınız...**
SEL loglarını indirilmek	**Download SEL Logs** üzerine tıklayın.
SEL loglarını silmek	**Clear SEL Logs** üzerine tıklayın.

Bölüm 7
Hizmet Yönetimi

İçindekiler Tablosu

7.1 Port Hizmet Parametrelerinin Yapılandırılması

Özet

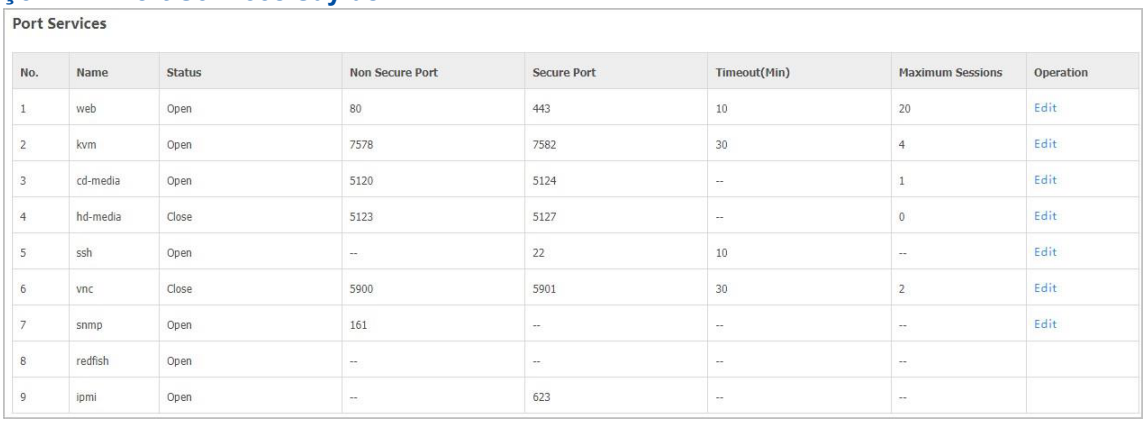
Port service parametrelerini yapılandırarak, BMC'nin herbir hizmeti için durum, güvenli port, güvenli olmayan port ve zaman aşımı parametrelerini yapılandırabilirsiniz.
Port Services sayfasında yapılandırılan parametreler, aşağıdaki sayfalarda yapılandırılan parametrelerle senkronize edilebilir:

- **Web Services** sayfası
- **Virtual Console** sayfası
- **Virtual Media** sayfası
- **VNC** sayfası
- **SNMP** sayfası

Adımlar

1. **Services'i** seçin. **Services** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Port Services** seçimini yapın. **Port Services** sayfası görüntülenir, bakınız Şekil 7-1.

Şekil 7-1 Port Services Sayfası



Port Services

No.	Name	Status	Non Secure Port	Secure Port	Timeout(Min)	Maximum Sessions	Operation
1	web	Open	80	443	10	20	Edit
2	kvm	Open	7578	7582	30	4	Edit
3	cd-media	Open	5120	5124	--	1	Edit
4	hd-media	Close	5123	5127	--	0	Edit
5	ssh	Open	--	22	10	--	Edit
6	vnc	Close	5900	5901	30	2	Edit
7	snmp	Open	161	--	--	--	Edit
8	redfish	Open	--	--	--	--	
9	ipmi	Open	--	623	--	--	

3. Parametreleri etkinleştirmek üzere bir hizmet için **Edit** üzerine tıklayın.
4. Parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 7-1'e başvurun.

Tablo 7-1 Port Service Parametre Açıklamaları

Parametre	Ayarlar
Status	Bir hizmetin etkinleştirilip etkinleştirilmeyeceğini seçin.
Non Secure Port	Hizmetin güvenli olmayan port numarasını girin. • Web servisinin güvenli olmayan varsayılan port numarası: 80. • KVM hizmetinin güvenli olmayan varsayılan port numarası: 7578. • CD medya servisinin varsayılan güvenli port numarası: 5120. • HD medya servisinin varsayılan güvenli port numarası: 5123. • VNC hizmetinin güvenli olmayan varsayılan port numarası: 5900. • SNMP hizmetinin güvenli olmayan varsayılan port numarası: 161. Diğer hizmetler güvenli olmayan portları desteklemez. Güvenli olmayan port numarası aralığı: 1–65535.
Secure Port	Hizmetin güvenli port numarasını girin. • Web servisinin varsayılan güvenli port numarası: 443. • KVM servisinin varsayılan güvenli port numarası: 7582. • CD ortam/medya hizmetinin varsayılan güvenli port numarası: 5124. • HD ortam/medya hizmetinin varsayılan güvenli port numarası: 5127. • SSH servisinin varsayılan güvenli port numarası: 22. • VNC servisinin varsayılan güvenli port numarası: 5901. • IPMI hizmetinin varsayılan güvenli port numarası: 623. Diğer hizmetler güvenli portları desteklemez. Güvenli port numarası aralığı: 1–65535.
Timeout(Min)	Hiçbir işlem gerçekleştirilmemişse hizmetin sonlandırılacağı zaman aşımı süresidir. Zaman aşımı süresini (dakika cinsinden) girin. Aralık: 5–30 (VNC hizmeti için) veya 1–30 (diğer hizmetler için).

Not

Maximum Sessions parametresini yapılandıramazsınız.

5. **Save** üzerine tıklayın.

7.2 Web Hizmet Parametrelerinin Yapılandırılması

Özet

Web hizmeti parametrelerini yapılandırarak, yerel PC üzerinden BMC'nin Web Portalına güvenli bir şekilde erişebilirsiniz.

Web hizmeti parametrelerini yapılandırmak için aşağıdaki işlemleri gerçekleştirin:

1. Temel parametrelerin yapılandırılması
2. Tarayıcıya SSL sertifikası yüklenmesi
3. SSL sertifikasının BMC'nin Web portalına yüklenmesi

Önkoşul

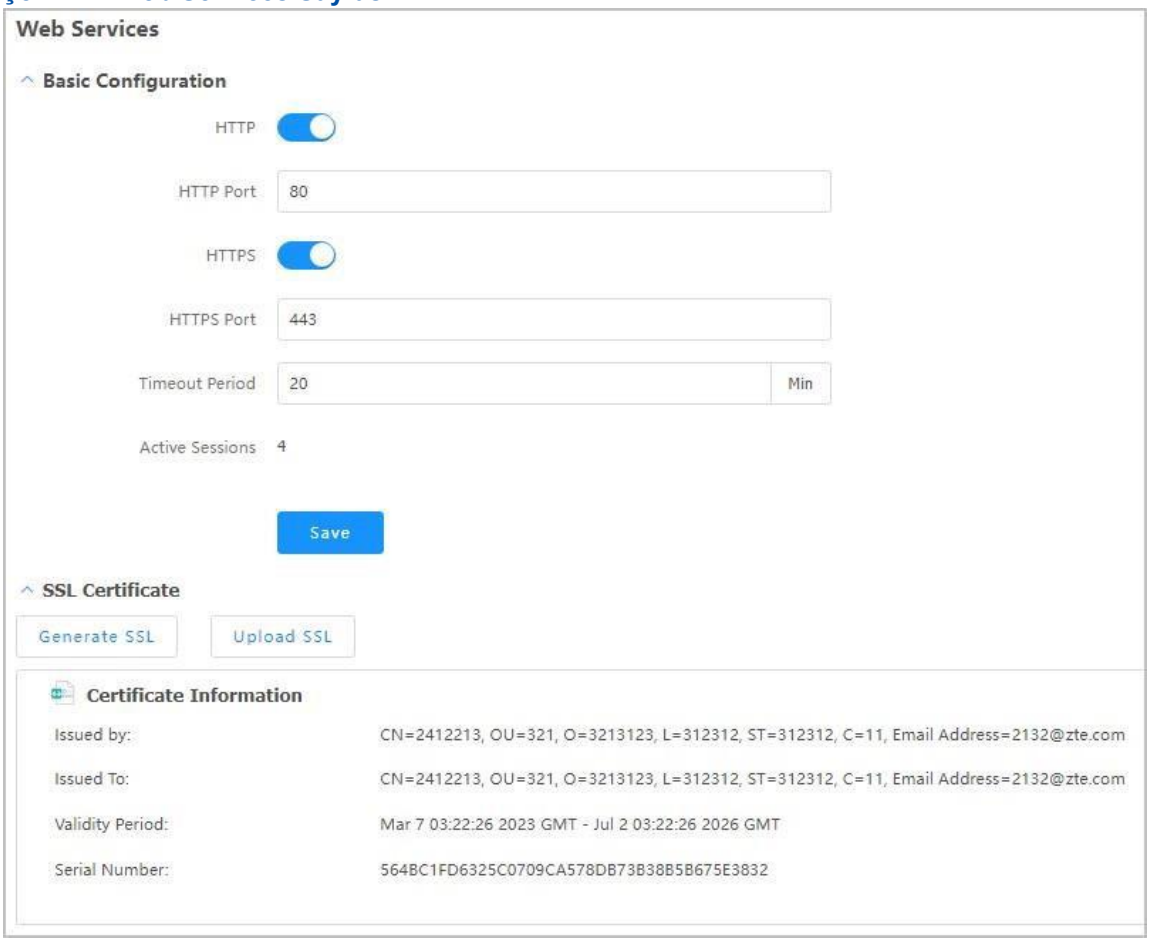
pem dosyası (sertifika dosyasını ve özel anahtar dosyasını içeren) halihazırda alınmış olmalıdır.

Adımlar

Temel Parametrelerin Yapılandırılması

1. BMC'nin Web portalında **Services**'i seçin. **Services** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Web Services** seçimini yapın. **Web Services** sayfası görüntülenir, bakınız Şekil 7-2.

Şekil 7-2 Web Services Sayfası



3. Parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 7-2'ye başvurun.

Tablo 7-2 Temel Parametre Açıklamaları

Parametre	Ayarlar
HTTP	**HTTP** anahtarını açın.
HTTP Port	Web hizmetinin güvenli olmayan port numarasını girin. Aralık: 1–65535, varsayılan: 80.
HTTPS	**HTTPS** anahtarını açın.
HTTPS Port	Web hizmetinin güvenli port numarasını girin. Aralık: 1–65535, varsayılan: 443.
Timeout Period	Belirlenen zaman aşımı süresi içinde hiçbir işlem yapılmazsa Web hizmeti sonlandırılır. Zaman aşımı süresini girin. Aralık: 1–30, birim: dakika.

Tarayıcıya SSL Sertifikası Yüklenmesi

4. PC'de tarayıcının **Settings** sayfasında (örneğin; Google Chrome) **Privacy and security** seçimini yapın.

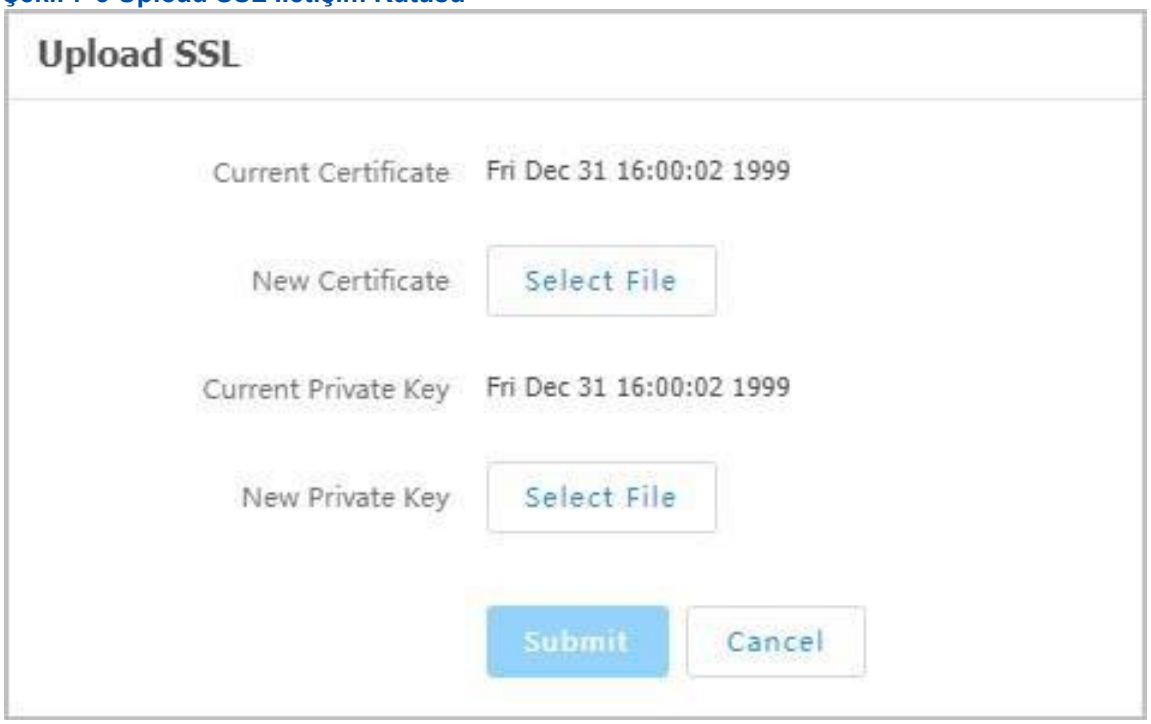
   . **Privacy and security** sayfası görüntülenir.

6. **Manage certificates'in** sağına tıklayın ve SSL sertifikasını yükleyin.

SSL Sertifikasının BMC'nin Web Portalına Yüklenmesi

7. BMC Web Portalının **Web Services** sayfasında **Upload SSL** üzerine tıklayın. **Upload SSL** iletişim kutusu görüntülenir, bakınız Şekil 7-3.

Şekil 7-3 Upload SSL İletişim Kutusu



8. Hazırlanmış olan sertifika dosyasını ve özel anahtar dosyasını seçin.
9. **Submit** üzerine tıklayın.

Doğrulama

Tarayıcınızın adres çubuğuna BMC'nin Web portalının adresini girin ve doğrudan login sayfasının görüntülendiğini ve "Not secure" (Güvenli değil) uyarısının görüntülenmediğini görmek için **Enter**'a basın, bakınız Şekil 7-4.

Şekil 7-4 Güvenli Erişim

Şekil 7-5'de tarayıcının adres çubuğunda görüntülenen "Not secure" (Güvenli değil) uyarısı gösterilmiştir.

Şekil 7-5 Güvenli Olmayan Erişim

7.3 KVM Hizmet Parametrelerinin Yapılandırılması

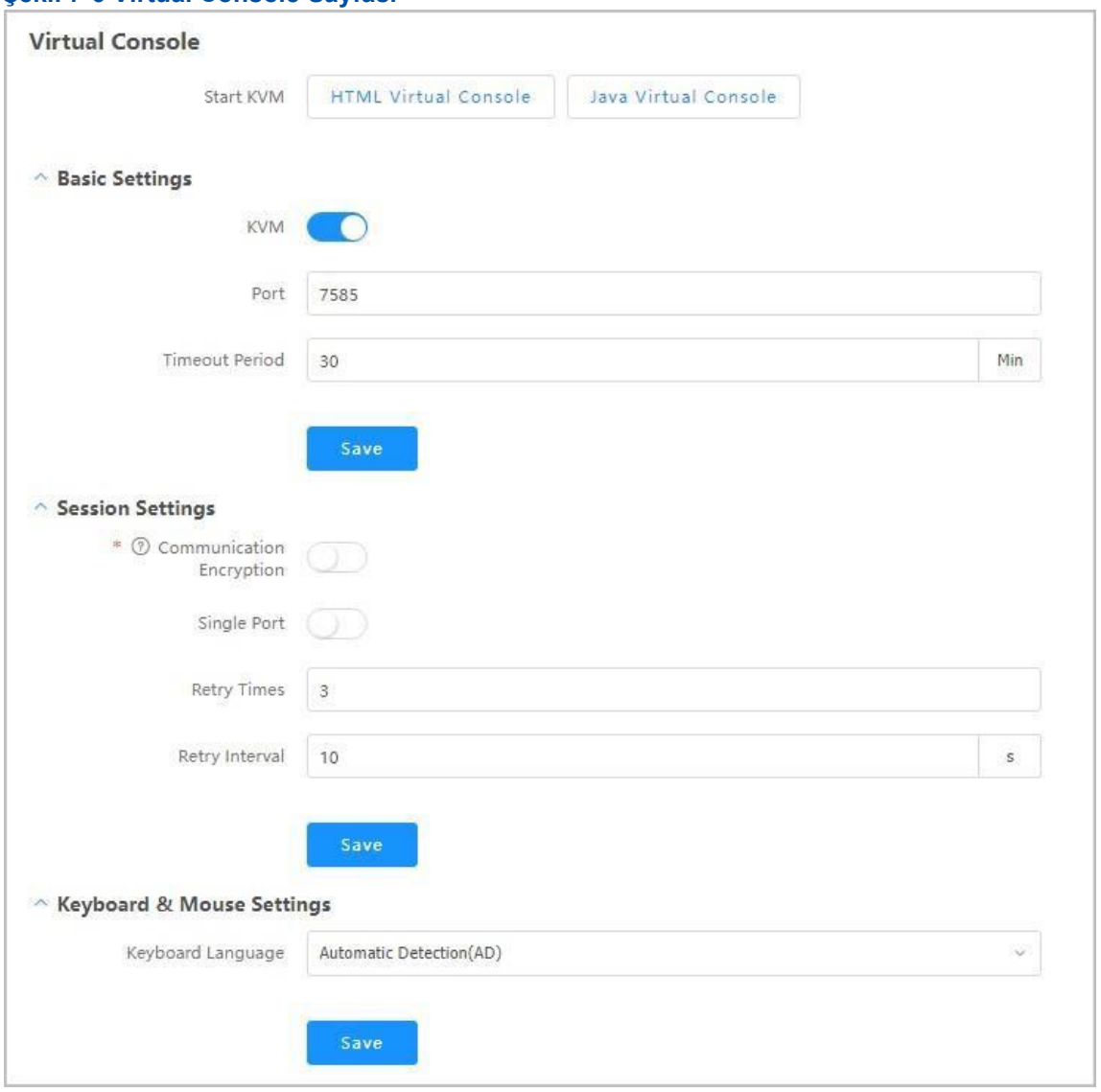
Özet

KVM'yi başlatmadan önce, KVM hizmet parametrelerini yapılandırmanız gerekir.

Adımlar

1. **Services'i** seçin. **Services** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Virtual Console** seçimini yapın. **Virtual Console** sayfası görüntülenir, bakınız Şekil 7-6.

Şekil 7-6 Virtual Console Sayfası



3. **Basic Settings** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 7-3'e başvurun.

Tablo 7-3 Basic Setting Parametre Açıklamaları

Parametre	Ayarlar
KVM	**KVM** anahtarını açın.
Port	KVM hizmetinin port numarasını girin. • Eğer **Session Settings** alanında **Communication Encryption** anahtarı kapalıysa, güvenli olmayan bir port numarası girin. • Eğer **Session Settings** alanında **Communication Encryption** anahtarı açıksa, güvenli bir port numarası girin.

Timeout Period	Belirlenen zaman aşımı süresi içinde hiçbir işlem yapılmazsa KVM hizmeti sonlandırılır.
Parametre	**Ayarlar**
	Zaman aşımı süresini girin. Aralık: 1–30, birim: dakika.

4. **Save** üzerine tıklayın.
5. **Session Settings** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 7-4'e başvurun.

Tablo 7-4 Session Setting Parametre Açıklamaları

Parametre	**Ayarlar**
Communication Encryption	KVM iletişiminin şifrelenip şifrelenmeyeceğini seçin.
Single Port	KVM, HTML modunda başlatıldığında 443 portunun birleşik bir şekilde kullanılıp kullanılmayacağını seçin. • Eğer **Single Port** anahtarı açıksa, 443 portu birleşik bir şekilde kullanılır. . • Eğer **Single Port** anahtarı kapalıysa, 443 portu birleşik bir şekilde kullanılmaz.
Retry Times	Oturum yeniden deneme sayısını girin. Aralık: 1–20.
Retry Interval	Oturum yeniden deneme aralığını girin. Aralık: 5–30, birim: saniye.

6. **Save** üzerine tıklayın.
7. **Keyboard & Mouse Settings** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 7-5'e başvurun.

Tablo 7-5 Keyboard & Mouse Setting Parametre Açıklamaları

Parametre	**Ayarlar**
Keyboard language	Uzak KVM için klavye dilini seçin.

8. **Save** üzerine tıklayın.

7.4 KVM'nin Başlatılması

Özet

Müşteri sahasında olmadığınızda, bir sunucuyu uzaktan kontrol etmek için KVM'yi başlatabilirsiniz.

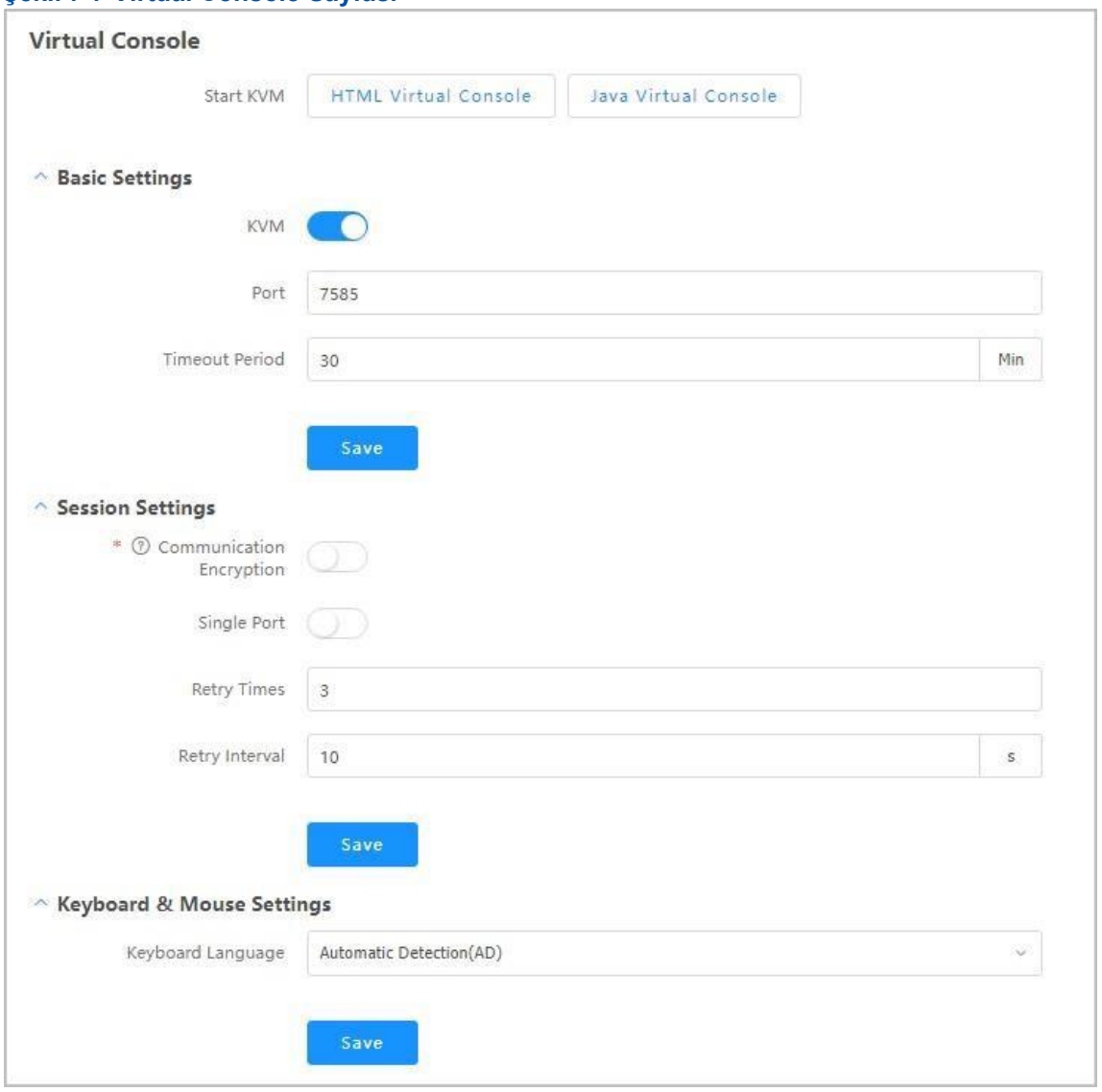
Önkoşul

Eğer KVM'nin Java modunda başlatılması gerekliyse, JRE 8 veya sonraki bir sürüm (örneğin, *jre- 8u191*) PC'ye halihazırda kurulmuş olmalıdır.

Adımlar

1. **Services'i** seçin. **Services** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Virtual Console** seçimini yapın. **Virtual Console** sayfası görüntülenir, bakınız Şekil 7-7.

Şekil 7-7 Virtual Console Sayfası



3. Aşağıdaki işlemleri gerektiği gibi gerçekleştirin.

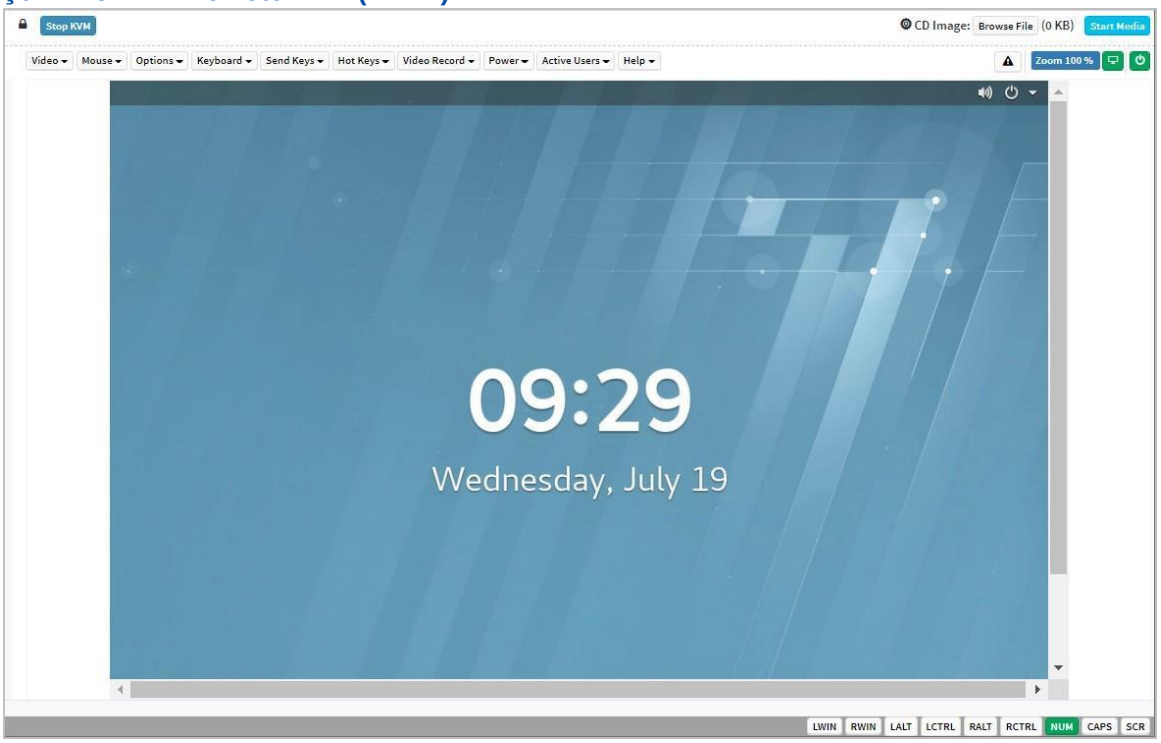
Aşağıdakileri gerçekleştirmek için...	Şunları yapınız...

KVM'nin HTML modunda başlatılması	a. **HTML Virtual Console** üzerine tıklayın. **Remote KVM (HTML)** sayfası görüntülenir, bakınız Şekil 7-8. b. Aşağıdaki işlemleri gerektiği gibi gerçekleştirin. İşlemlere dair açıklamalar için, Tablo 7-6'ya bakın.
KVM'nin Java modunda başlatılması	a. PC'nin sol alt köşesindeki arama kutusuna `Java` girin. b. Arama sonuçları arasından **Java'yı** seçin. **Java Control Panel** iletişim kutusu görüntülenir. c. **Security** üzerine tıklayın. **Security** penceresi görüntülenir.
Aşağıdakileri gerçekleştirmek için...	**Şunları yapın...**
	d. **Edit Site List** üzerine tıklayın. **Exception Site List** iletişim kutusu görüntülenir. e. BMC Web portalının adresini eklemek için **Add** üzerine tıklayın. f. **Security** penceresine dönmek için **OK** üzerine tıklayın. g. **OK** üzerine tıklayın. h. BMC Web Portalının **Virtual Console** sayfasında **Java Virtual Console** üzerine tıklayın. `jviewer.jnlp'yi` saklamak isteyip istemediğinize dair bir iletişim kutusu görüntülenir. i. **Keep** üzerine tıklayın. j. Tarayıcının sol alt köşesinde `jviewer.jnlp` üzerine tıklayın. Devam etmek isteyip istemediğinize dair bir iletişim kutusu görüntülenir. k. **Continue** üzerine tıklayın. **Do you want to run this application?** iletişim kutusu görüntülenir. l. **I accept the risk and want to continue to run this app.** seçeneğini seçin ve **Run** üzerine tıklayın. **Untrusted Connection** iletişim kutusu görüntülenir. m. **Yes** üzerine tıklayın. **Remote KVM (JAVA)** sayfası görüntülenir, bakınız Şekil 7-9. n. Aşağıdaki işlemleri gerektiği gibi gerçekleştirin. İşlemlere dair açıklamalar için, Tablo 7-7'ye bakın.

Not

KVM'yi bir modda başlatmadan önce, KVM'yi diğer modda devre dışı bırakmanız gerekir. Örneğin; KVM'yi Java modunda başlatmadan önce HTML modunda başlatılmış olan KVM'yi devre dışı bırakmanız gerekir.

Şekil 7-8 Remote KVM (HTML)



Tablo 7-6 Remote KVM (HTML) İşlemlerinin Açıklamaları

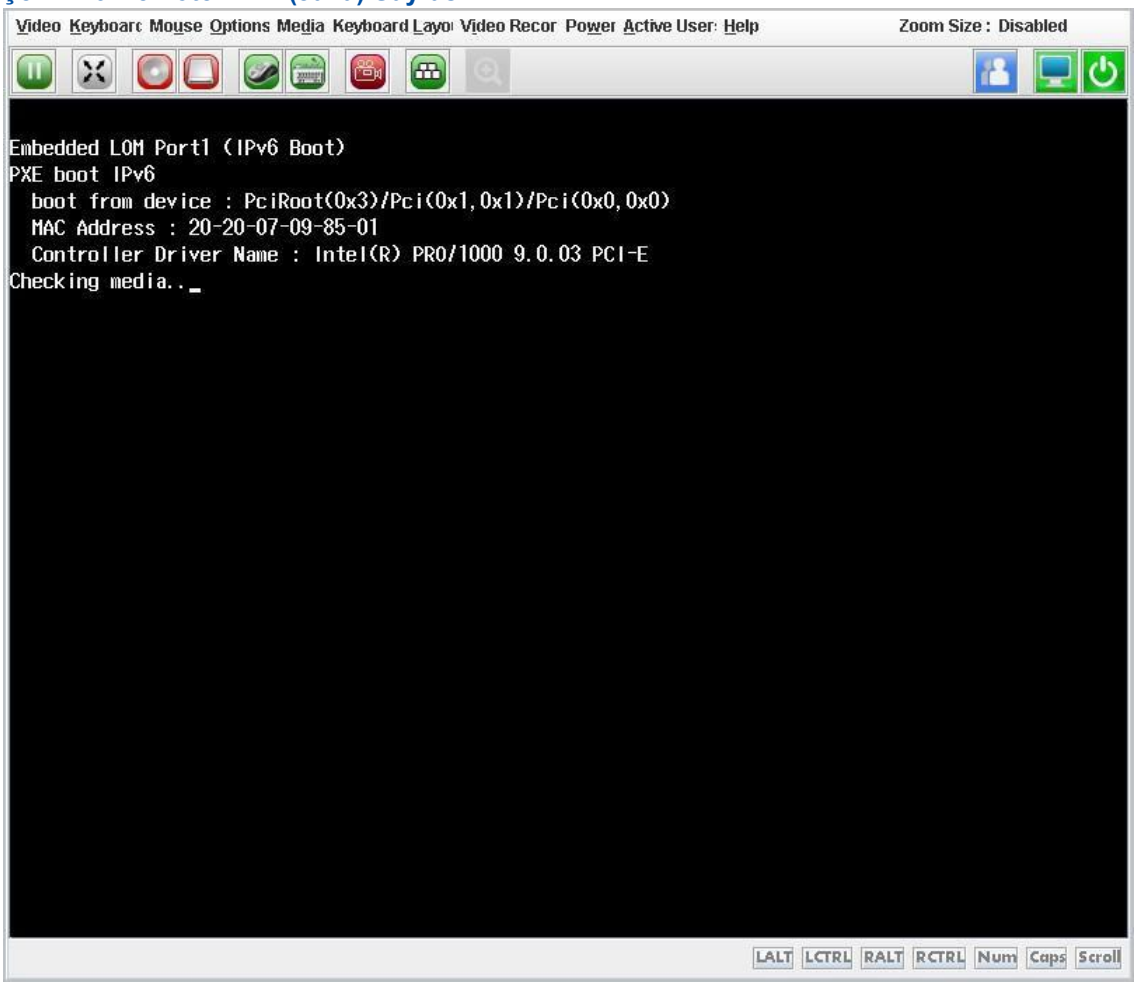
İşlem	Açıklama
KVM'nin durdurulması	**Remote KVM (HTML)** sayfasından çıkmak için **Stop KVM** üzerine tıklayın.
Yerel bir `iso` dosyasının tanıtılması	a. **CD Image'nin** yanındaki **Browse File** üzerine tıklayın ve PC'den `iso` dosyasını seçin. b. **Start Media** üzerine tıklayın.
Alınan bildirimlerin görüntülenmesi	simgesine tıklayın.
Sunucunun ekranının kilitlenmesi	Sunucu ekranını aşağıdaki yollardan birini kullanarak kilitleyin: • simgesine tıklayın. • **Video > Display OFF** seçimini yapın. Sunucu ekranı kilitlendikten sonra, eğer başka bir kullanıcı bir sunucu ekranı görüntülemek isterse, geçerli aktif kullanıcıya bir izin isteği gönderilir. Kullanıcı sadece geçerli aktif kullanıcı tarafından yetkilendirildikten sonra sunucu ekranını görüntüleyebilir.

Sunucu ekranının kilidinin açılması	Sunucu ekranının kilidini aşağıdaki yollardan birini kullanarak açın: •  simgesine tıklayın. • **Video > Display ON** seçimini yapın.  Simgesi,  simgesine dönüşür.

İşlem	**Açıklama**
Bir uzaktan kontrol ekranının duraklatılması	**Video > Pause Video** seçimini yapın.
Bir uzaktan kontrol ekranının yeniden başlatılması	**Video > Resume Video** seçimini yapın.
Bir uzaktan kontrol ekranının yenilenmesi	**Video > Refresh Video** seçimini yapın.
Geçerli ekranın yakalanması	**Video > Capture Screen** seçimini yapın.
Sunucu ekranlarındaki fare imlecinin gösterilmesi veya gizlenmesi	• Sunucu ekranlarında fare imlecini göstermek için **Mouse'a** tıklayın ve **Show Client Cursor** seçimini yapın. • Sunucu ekranlarında fare imlecini gizlemek için **Mouse'a** tıklayın ve **Show Client Cursor** seçimini kaldırın.
Fare modunun ayarlanması	**Mouse'a** tıklayın ve **Absolute Mouse Mode** seçimini yapın. Absolute mouse modunda, sunucudaki fareyi hareket ettirmek için yerel farenin mutlak konumu sunucuya aktarılır.
Klavye düzeninin ayarlanması	a. **Keyboard'u** seçin. b. Görüntülenen alt menüde **English U.S, German** ve **Japanese** dahil olmak üzere klavye düzenini seçin . Varsayılan olarak **English U.S** seçilidir. .
Video kaydetme süresi uzunluğunun ayarlanması	a. **Video Record > Record Settings** seçimini yapın. **Record Settings** iletişim kutusu görüntülenir. b. 1–1800 saniye aralığında olacak şekilde video kaydetme süresi uzunluğunu seçin. c. **OK** üzerine tıklayın.
Videoların kaydedilmesi	**Video Record > Record Video** seçimini yapın.
Kaydın durdurulması	**Video Record > Stop Recording** seçimini yapın.
Sunucunun kapatılması	Aşağıdaki yollardan birini kullanarak sunucuyu kapatın: • **Power > Orderly shutdown** seçimini yapın. •  simgesine tıklayın.

Sunucunun başlatılması	Aşağıdaki yollardan birini kullanarak sunucuyu başlatın: • **Power > Power On Server** seçimini yapın. •  simgesine tıklayın.
Bir cold reboot işleminin gerçekleştirilmesi	**Power > Power Cycle Server** seçimini yapın. Cold reboot, sunucunun kapatıldıktan sonra başlatıldığı anlamına gelir. Yeniden başlatma esnasında sunucu çevrimdışıdır.
Warm reboot işleminin gerçekleştirilmesi	**Power > Reset Sunucu** seçimini yapın. Warm reboot, sunucunun kapalı değilken yeniden başlatıldığı anlamına gelir. Yeniden başlatma esnasında sunucu çevrimdışı değildir.
İşlem	**Açıklama**
Uzaktan kontrol özelliğini kullanan kullanıcıların görüntülenmesi	**Active Users** seçimini yapın.

Şekil 7-9 Remote KVM (Java) Sayfası



Tablo 7-7 Remote KVM (JAVA) İşlemlerinin Açıklamaları

İşlem	Açıklama
Bir uzaktan kontrol ekranının duraklatılması	Aşağıdaki yollardan birisi ile uzaktan kontrol ekranını duraklatın: • **Video > Pause Redirection** seçimini yapın. •  simgesine tıklayın. • **Alt+P** üzerine basın.
Bir uzaktan kontrol ekranının yeniden başlatılması	Aşağıdaki yollardan birisi ile uzaktan kontrol ekranını yeniden başlatın: • **Video > Resume Redirection** seçimini yapın. •  simgesine tıklayın. • **Alt+R** üzerine basın.

İşlem	Açıklama
Bir uzaktan kontrol ekranının yenilenmesi	Aşağıdaki yollardan herhangi birisi ile uzaktan kontrol ekranını yenileyin: • **Video > Refresh Video** seçimini yapın. • **Alt+E** üzerine basın.
Host ekranı görüntüleme moduna geçiş .	• Host üzerinde uzak ekranı görüntülemek için **Video > Turn ON Host Display** seçimini yapın. • Host üzerinde uzak ekranı görüntülememek için **Video > Turn OFF Host Display** seçimini yapın. Not: Hostun uzak ekran görüntüleme modları arasında hızlı geçiş yapmak için aşağıdaki yöntemlerden herhangi birisini kullanabilirsiniz. •  simgesine tıklayın. • **Alt+N** üzerine basın.
Geçerli ekranın yakalanması	Aşağıdaki yollardan birini kullanarak geçerli ekranı yakalayın: • **Video > Capture Screen** seçimini yapın. • **Alt+S** üzerine basın.
Bir video kod çözme (decoding) modunun ayarlanması	a. **Video > Compression Mode** seçimini yapın. b. Görüntülenen alt menüden bir video kod çözme (decoding) modu seçin.
Video görüntü kalitesinin ayarlanması	a. **Video > DCT Quantization Table** seçimini yapın. b. Görüntülenen alt menüden video görüntü kalitesini seçin. Video görüntü kalitesi; video kalitesinin sırayla düştüğü 0 ila 7 aralığındaki sekiz seviyeye bölünür

Bir tuş kombinasyonu tanımlanması	a. **Keyboard > Hot Keys > add Hot Keys** seçimini yapın. **User Defined Macros** sayfası görüntülenir. b. **Add** üzerine tıklayın. **Add Macros** sayfası görüntülenir. c. Kullanıcı tarafından tanımlanan tuş kombinasyonuna basın ve ardından bırakın. d. **OK** üzerine tıklayın.
Tam klavye desteğinin etkinleştirilmesi	• Tam klavye desteğini etkinleştirmek için **Keyboard**'a tıklayın ve **Full Keyboard Support** seçimini yapın. • Tam klavye desteğini devre dışı bırakmak için **Keyboard**'a tıklayın ve **Full Keyboard Support** seçimini kaldırın.
Fare imlecinin gösterilmesi veya gizlenmesi	• Sunucu ekranlarında fare imlecini göstermek için **Mouse'a** tıklayın ve **Show Client Cursor** seçimini yapın. • Fare imlecini gizlemek için **Mouse'a** tıklayın ve **Show Client Cursor** seçimini kaldırın. PC'de fare imlecini görüntüleme modlarını hızlı bir şekilde değiştirmek için aşağıdaki yöntemlerden herhangi birisini kullanabilirsiniz. • **Alt+C** üzerine basın. •  simgesine tıklayın.
Şebeke bant genişliğinin ayarlanması	a. **Options > Bandwidth** seçimini yapın.

İşlem	**Açıklama**
	b. Görüntülenen alt menüden istenen ağ bant genişliğini seçin.
Farenin/klavyenin şifreleme durumun değiştirilmesi	• Fare/klavye şifrelemenin etkinleştirilmesi için **Options** üzerine tıklayın ve **Keyboard/Mouse Encryption** seçimini yapın. • Fare/klavye şifrelemenin devre dışı bırakılması için **Options** üzerine tıklayın ve **Keyboard/Mouse Encryption** seçimini kaldırın.
Bir uzak ekranın ölçekleme modunun ayarlanması	a. **Options > Zoom** seçimini yapın. b. Görüntülenen alt menüde, uzak ekranın yakınlaştırma/uzaklaştırma ölçeğini ayarlayın. • **Zoom In**: uzak ekranı yakınlaştırır. • **Zoom Out**: uzak ekranı uzaklaştırır. • **Actual Size**: uzak ekranı %100 oranında görüntüler. • **Fit to Client Resolution**: uzak ekranı yerel istemci sisteminin çözünürlüğünde görüntüler. • **Fit to Host Resolution**: uzak ekranı uzak sunucu sisteminin çözünürlüğünde görüntüler.

Sunucuya bir IPMI komutunun gönderilmesi	a. **Options > Send IPMI Command** seçimini yapın. **IPMI Command Dialog** penceresi görüntülenir . b. IPMI komutunu girin. c. **Send** üzerine tıklayın. IPMI komutu; hex ve ASCII formatlarını destekler.
GUI dilinin ayarlanması	a. **Options > GUI Languages** seçimini yapın. b. Görüntülenen alt menüden GUI dilini seçin.
Ayrıcalık talebi modunun ayarlanması	a. **Options > Block Privilege Request** seçimini yapın. b. Görüntülenen alt menüden bir ayrıcalık talebi engelleme modu seçin. • **Allow only Video**: Bir ayrıcalık isteği başlatan kullanıcıya otomatik olarak, sunucuda görüntülenen bilgileri görüntüleme izni verilir. • **Deny Access**: Sistemdeki ayrıcalık talepleri engellenir.
Yerel bir `iso` dosyasının tanıtılması	a. Aşağıdaki yollardan herhangi birisini kullanarak **Virtual Media** penceresini açın: • **Media > Virtual Media Wizard...** seçimini yapın ve **CD/DVD** sekmesine geçin. •  simgesine tıklayın. b. **Browse** üzerine tıklayın ve bir yerel `iso` dosyası seçin. c. **Connect** üzerine tıklayın.
Bir yerel dizinin tanıtılması	a. PC'de bir `iso` dosyası oluşturun. b. Aşağıdaki yollardan herhangi birisini kullanarak **Virtual Media** penceresini açın: • **Media > Virtual Media Wizard...** seçimini yapın ve **Hard Disk/USB** sekmesine geçin. •  simgesine tıklayın . c. **physical drive > folder path** seçimini yapın.

İşlem	**Açıklama**
	d. **Browse** üzerine tıklayın ve bir yerel klasör yolu seçin. e. **Size** ve **folder path'i** ayarlayın. f. **Connect** üzerine tıklayın. **Size** değeri 2, 4 ve 8 gibi bir 2^n değeri olmalıdır. **folder path** ile belirlenen yolun yeni `iso` dosyasınınki ile aynı olması gereklidir.
Klavye düzeninin ayarlanması	a. **Keyboard Layout'u** seçin. b. Görüntülenen alt menüden klavye düzenini seçin.
Dokunmatik klavyenin açılması	 simgesine tıklayın.

Video kaydının yapılandırılması	a. **Video Record > Settings** seçimini yapın. **Video Record** penceresi görüntülenir. b. Video kaydetme süresi uzunluğunu saniye cinsinden belirleyin ve video depolama konumunu belirleyin. c. **OK** üzerine tıklayın. Video kaydetme süresi uzunluğu, 1 ila 1800 saniye aralığında değişir.
Videoların kaydedilmesi	a. Aşağıdaki yollardan herhangi birisini kullanarak bir video kaydetmeye başlayın: • **Video Record > Start Record** seçimini yapın. •  simgesine tıklayın. b. (Opsiyonal) Aşağıdaki yollardan birini kullanarak video kaydetmeyi durdurun: • **Video Record > Stop Record** seçimini yapın. •  simgesine tıklayın. c. Önceden belirlenmiş kaydetme süresi uzunluğuna erişildiğinde veya kaydetme manuel olarak durdurulduktan sonra, **OK** üzerine tıklayın. Kaydedilen video dosyası, önceden belirlenmiş `VideoCaptures` klasörüne kaydedilir.
Sunucu güç modunun ayarlanması	a. **Power'ı** seçin. b. Görüntülenen alt menüden bir sunucu gücü seçeneği seçin. Sunucu gücü seçenekleri aşağıdaki gibidir: • **Reset Server**: güç kaynağını kapatmadan sistemi yeniden başlatır (warm reboot). • **Immediate Shutdown**: güç kaynağını kapatarak, sunucuyu derhal kapatır. • **Orderly Shutdown**: sunucuyu program kontrolü vasıtasıyla usule uygun olarak kapatır. • **Power On Server**: sunucuyu başlatır. • **Power Cycle Server**: sunucuyu kapatır ve yeniden başlatır (cold reboot).
Aktif kullanıcıların kontrol edilmesi	Aşağıdaki yollardan herhangi birisi ile uzaktan kontrol kullanarak kullanıcıları görüntüleyin: • **Active Users** seçimini yapın. •  simgesine tıklayın.

7.5 Virtual Media Parametrelerinin Yapılandırılması

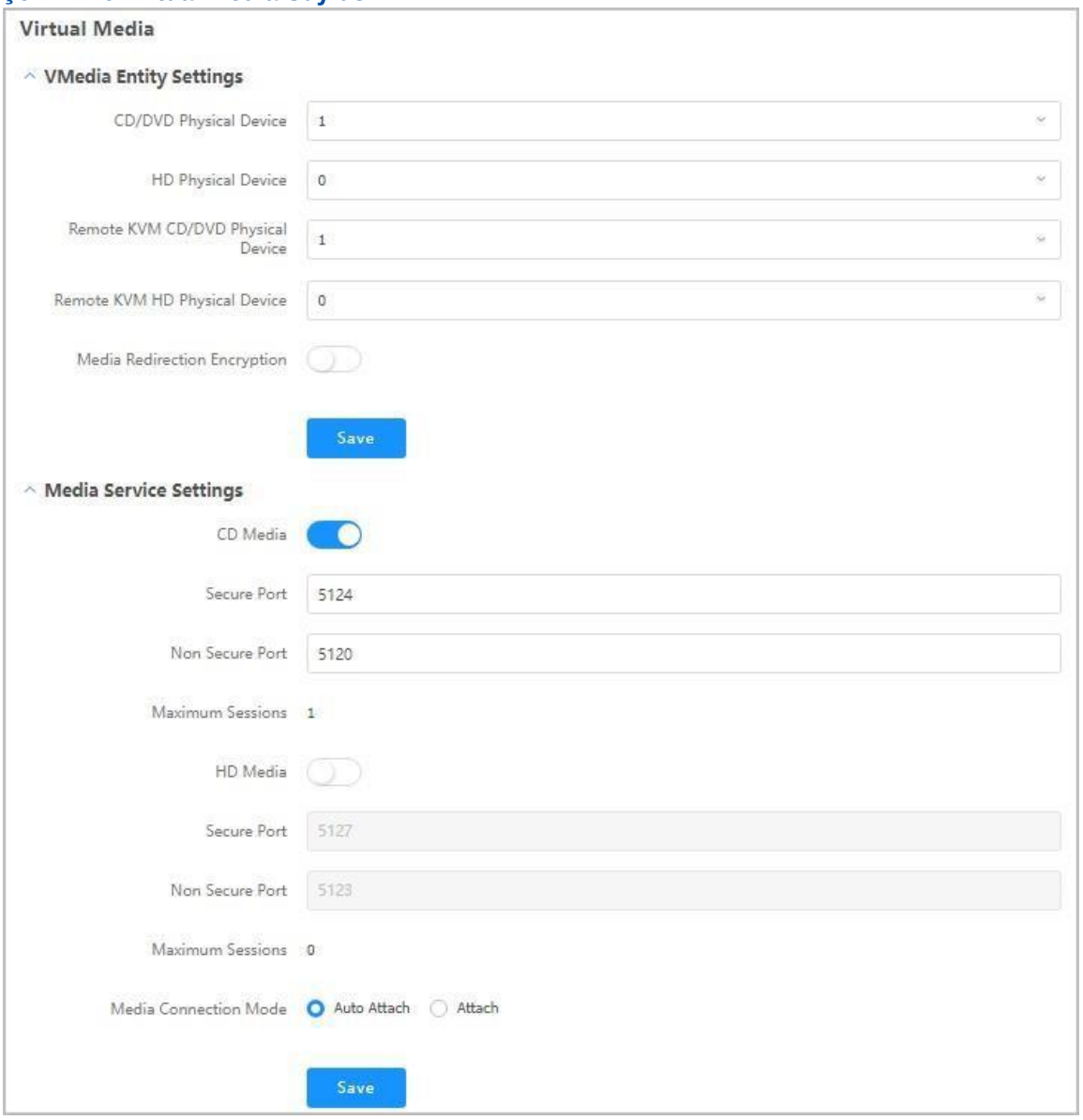
Özet

KVM üzerinden PC'nin bir CD/DVD veya HD'sini sunucuya monte etmeden VMedia instance parametrelerini yapılandırmanız gereklidir.

Adımlar

1. **Services'i** seçin. **Services** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Virtual Media** seçimini yapın. **Virtual Media** sayfası görüntülenir, bakınız Şekil 7-10.

Şekil 7-10 Virtual Media Sayfası



3. **VMedia Entity Settings** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 7-8'e başvurun.

Tablo 7-8 VMedia Instance Settings Parametre Açıklamaları

Parametre	Ayarlar

CD/DVD Fiziksel Cihaz	PC'de CD/DVD cihazlarının sayısını seçin. Varsayılan değer olan **1'i** tutun.
HD Fiziksel Cihaz	PC'de HD cihazlarının sayısını seçin. Varsayılan değer olan **0'ı** tutun.
Uzak KVM CD/DVD Fiziksel Cihazı	KVM üzerinden monte edilecek CD/DVD cihazlarının sayısını seçin. Varsayılan değer olan **1'i** tutun.
Uzak KVM HD Fiziksel Cihazı	KVM üzerinden monte edilecek HD cihazlarının sayısını seçin. Varsayılan değer olan **0'ı** tutun.
Ortam (Medya) Yeniden Yönlendirme Şifrelemesi	**Media Redirection Encryption** anahtarını kapatın.

4. **Save** üzerine tıklayın.
5. **Media Service Settings** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 7-9'a başvurun.

Tablo 7-9 Media Service Settings Parametre Açıklamaları

Parametre	**Ayarlar**
CD Media	• CD media hizmetinin etkinleştirilmesi için **CD Media** anahtarını açın. • CD media hizmetinin devre dışı bırakılması için **CD Media** anahtarını kapatın.
Secure Port	Bu parametre **CD Media** anahtarı açıldığında ayarlanabilir. CD media hizmetinin güvenli port numarasını girin. Aralık: 1–65535, varsayılan: 5124.
Non Secure Port	Bu parametre **CD Media** anahtarı açıldığında ayarlanabilir. CD media hizmetinin güvenli olmayan port numarasını girin. Aralık: 1–65535, varsayılan: 5120.
HD Media	• HD media hizmetinin etkinleştirilmesi için **HD Media** anahtarını açın. • HD media hizmetinin devre dışı bırakılması için HD Media anahtarını kapatın.
Secure Port	Bu parametre **HD Media** anahtarı açıldığında ayarlanabilir. HD media hizmetinin güvenli port numarasını girin. Aralık: 1–65535, varsayılan: 5127.
Non Secure Port	Bu parametre **HD Media** anahtarı açıldığında ayarlanabilir. HD media hizmetinin güvenli olmayan port numarasını girin. Aralık: 1–65535, varsayılan: 5123.
Media Connection Mode	Arzu edilen ortam (medya) bağlantı modu seçin. • **Auto Attach**: otomatik olarak yeniden bağlanır.
Parametre	**Ayarlar**

	• **Attach**: otomatik olarak yeniden bağlanmaz.

6. **Save** üzerine tıklayın.

7.6 VNC Parametrelerinin Yapılandırılması

Özet

Bir sunucu, KVM ve VNC üzerinden uzaktan kontrol edilebilir. Sunucuyu VNC modundan uzaktan kontrol etmeden önce VNC parametrelerini yapılandırmanız gereklidir.

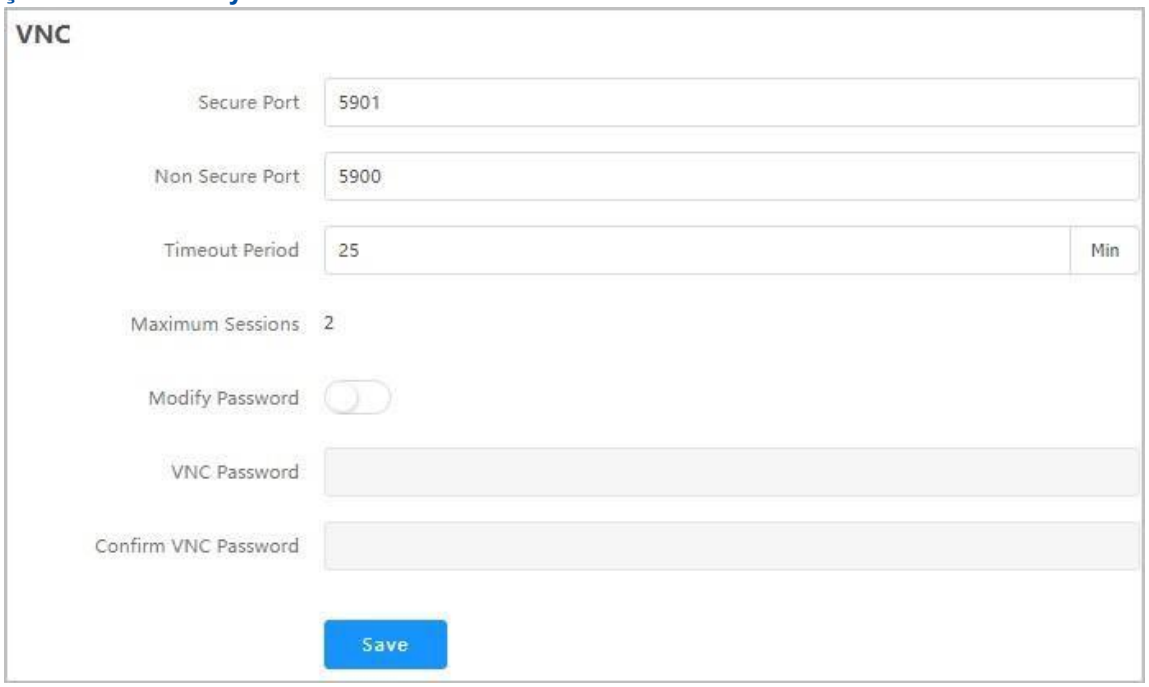
Not

KVM ile ilgili parametre yapılandırması hakkında bilgi almak için 7.3 KVM Hizmet Parametrelerinin Yapılandırılması bölümüne başvurun. KVM tabanlı uzaktan sunucu kontrolü işlemleri hakkında bilgi almak için 7.4 KVM'nin Başlatılması bölümüne başvurun.

Adımlar

1. **Services'i** seçin. **Services** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **VNC** seçimini yapın. **VNC** sayfası görüntülenecektir, bakınız Şekil 7-11.

Şekil 7-11 VNC Sayfası



3. Parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 7-10'a başvurun.

Tablo 7-10 VNC Parametre Açıklamaları

Parametre	Ayarlar
Secure Port	VNC hizmetinin güvenli port numarasını girin. Aralık: 1–65535, varsayılan: 5901.
Non Secure Port	VNC hizmetinin güvenli olmayan port numarasını girin. Aralık: 1–65535, varsayılan: 5900.
Timeout Period	Belirlenen zaman aşımı süresi içinde hiçbir işlem yapılmazsa VNC hizmeti sonlandırılır. Zaman aşımı süresini girin. Aralık: 5–30, birim: dakika.
Modify Password	VNC parolasının değiştirilip değiştirilmeyeceğine karar vermek için aşağıdakileri gerçekleştirin. • VNC parolasını değiştirmek için **Modify Password** anahtarını açın. • VNC parolasını değiştirmemek için **Modify Password** anahtarını kapatın. .
VNC Password	Bu parametre **Modify Password** anahtarı açıldığında ayarlanabilir. Yeni VNC parolasını girin. Bir VNC parolası; rakamlar, harfler ve boşluk hariç özel karakterler içerir ve en fazla sekiz karakterden oluşur. Bu parametre boş bırakılırsa, varsayılan parola geri yüklenir.
Confirm VNC Password	Bu parametre **Modify Password** anahtarı açıldığında ayarlanabilir. **VNC Password** ile aynı olması gereken yeni VNC parolasını onaylayın.

4. **Save** üzerine tıklayın.

7.7 SNMP Parametrelerinin Yapılandırılması

Özet

Bu prosedürde, BMC ve bir üçüncü taraf NMS arasındaki iletişim için SNMP parametrelerinin nasıl yapılandırılacağı açıklanmıştır.

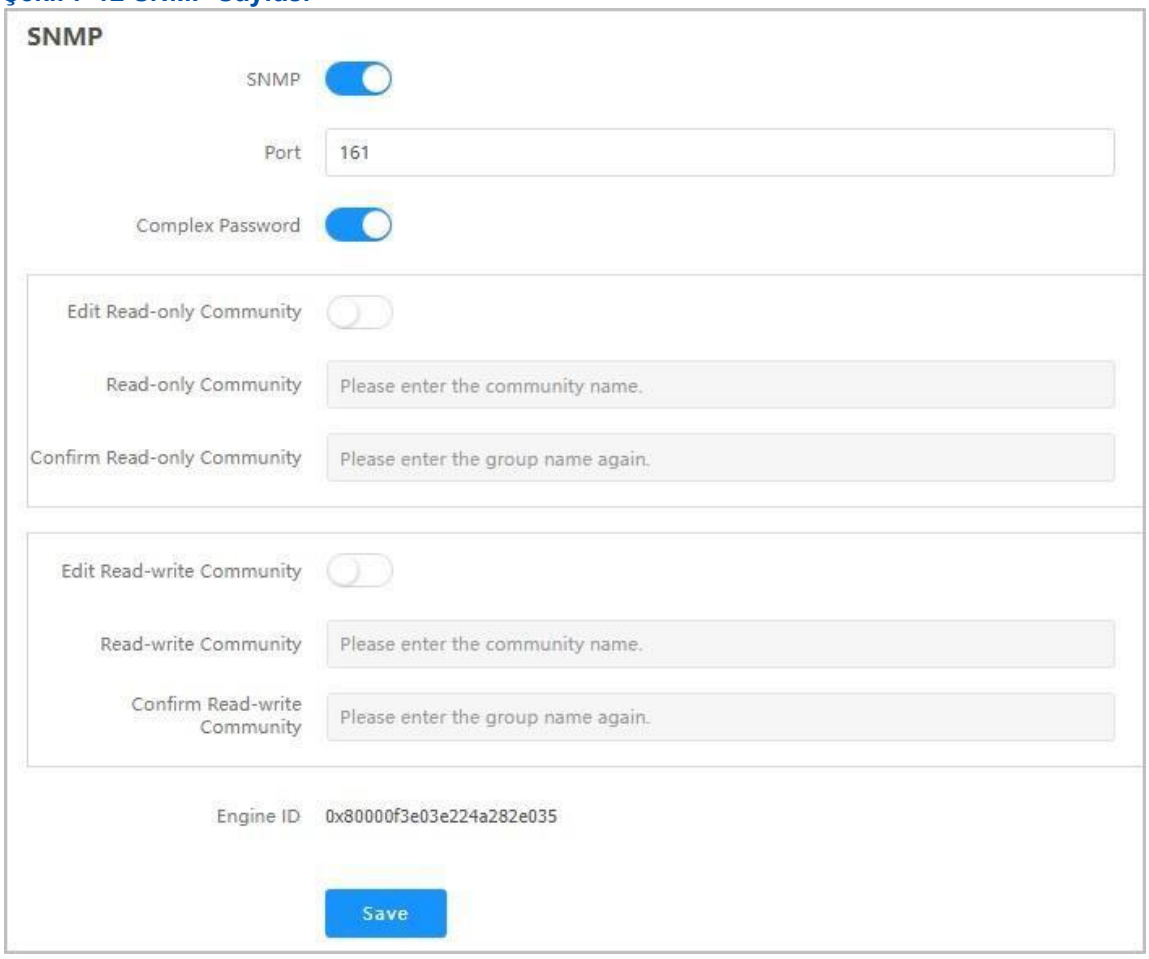
Not

SNMP parametreleri, üçüncü taraf NMS'i tarafından sağlanır, dolayısıyla BMC'nin Web portalında ayarlanan SNMP parametrelerinin değerleri, üçüncü taraf NMS'indeki parametrelerin değerleriyle aynı olmalıdır.

Adımlar

1. **Services'i** seçin. **Services** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **SNMP** seçimini yapın. **SNMP** sayfası görüntülenecektir, bakınız Şekil 7-12.

Şekil 7-12 SNMP Sayfası



3. Parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 7-11'e başvurun.

Tablo 7-11 SNMP Parametre Açıklamaları

Parametre	Ayarlar
SNMP	**SNMP** anahtarını açın.
Port	SNMP hizmetinin güvenli olmayan port numarasını girin. Aralık: 1–65535, varsayılan: 161.

Complex Password	Karmaşık parola işlevinin etkinleştirilip etkinleştirilmeyeceğine karar vermek için aşağıdakileri gerçekleştirin. • Karmaşık parola işlevini etkinleştirmek için **Complex Password** anahtarını açın. • Karmaşık parola işlevini devre dışı bırakmak için **Complex Password** anahtarını kapatın.
Edit Read-only Community	Salt okunur topluluk adının düzenlenip düzenlenmeyeceğine karar vermek için aşağıdakileri gerçekleştirin. • Salt okunur topluluk adını düzenlemek için **Edit Read-only Community** anahtarını açın. • Salt okunur topluluk adını düzenlememek için **Edit Read-only Community** anahtarını kapatın.
Parametre	**Ayarlar**
Read-only Community	Bu parametre **Edit Read-only Community** anahtarı açıldığında ayarlanabilir. Salt okunur topluluk adını girin (varsayılan: roAdmin9!).
Confirm Read-only Community	Bu parametre **Edit Read-only Community** anahtarı açıldığında ayarlanabilir. Belirlenen **Read-only Community** ile aynı olması gereken salt okunur topluluk adını onaylayın.
Edit Read-write Community	Okuma-yazma topluluk adının düzenlenip düzenlenmeyeceğine karar vermek için aşağıdakileri gerçekleştirin. • Okuma-yazma topluluk adını düzenlemek için **Edit Read-write Community** anahtarını açın. • Okuma-yazma topluluk adını düzenlememek için **Edit Read-write Community** anahtarını kapatın.
Read-write Community	Bu parametre **Edit Read-write Community** anahtarı açıldığında ayarlanabilir. Okuma-yazma topluluk adını girin (varsayılan: rwAdmin9!).
Confirm Read-write Community	Bu parametre **Edit Read-write Community** anahtarı açıldığında ayarlanabilir. Belirlenen **Read-write Community** ile aynı olması gereken okuma-yazma topluluk adını onaylayın.

4. **Save** üzerine tıklayın.

Bölüm 8
BMC Yönetimi

İçindekiler Tablosu

8.1 Ağ Parametresi Yapılandırma

8.1.1 Host Adının Yapılandırılması

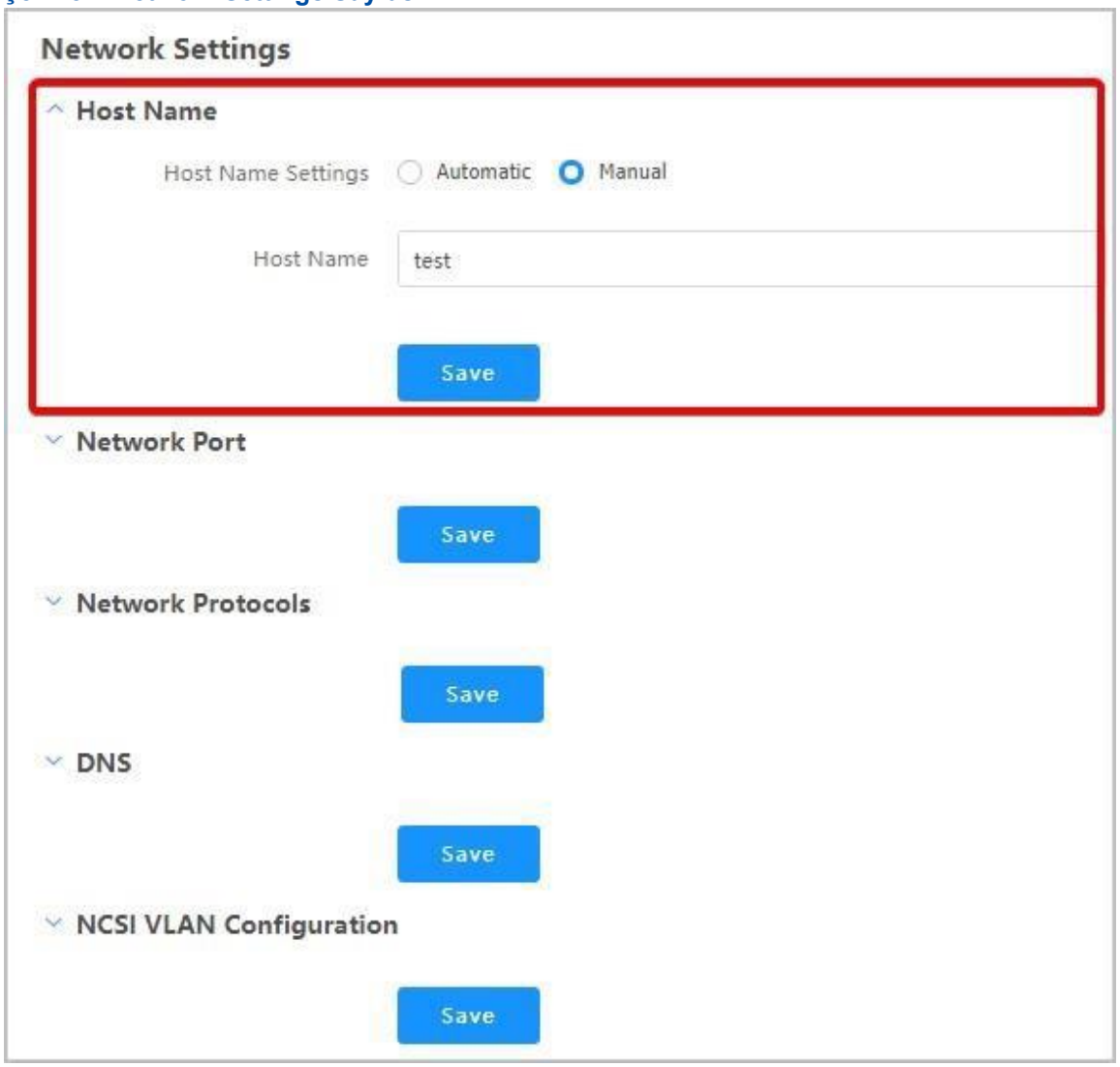
Özet

Bu prosedürde, sunucuyu tanımlamak için host adının nasıl yapılandırılacağı açıklanmıştır.

Adımlar

1. **BMC Settings'i** seçin. **BMC Settings** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Network Settings** seçimini yapın. **Network Settings** sayfası görüntülenir, bakınız Şekil 8-1.

Şekil 8-1 Network Settings Sayfası



3. **Host Name** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 8-1'e başvurun.

Tablo 8-1 Host Name Parametre Açıklamaları

Parametre	Ayarlar
Host Name Settings	Arzu edilen host adı ayarını seçin. • **Automatic**: Sistem tarafından otomatik olarak bir host adı belirlenir. • **Manual**: **Host Name** metin kutusuna bir host adının manuel olarak girilmesi gerekir.
Host Name	**Host Name Settings** değeri **Manual** olarak ayarlandıysa bu parametre gereklidir. Host adını girin. Bir host adı; rakamlar, harfler ve kısa çizgiler (-) içerir ve en fazla 64 karakterden oluşur. Host adı kısa çizgi ile başlayamaz veya bitemez.

4. **Save** üzerine tıklayın.

8.1.2 Ağ Portu Modunun Yapılandırılması

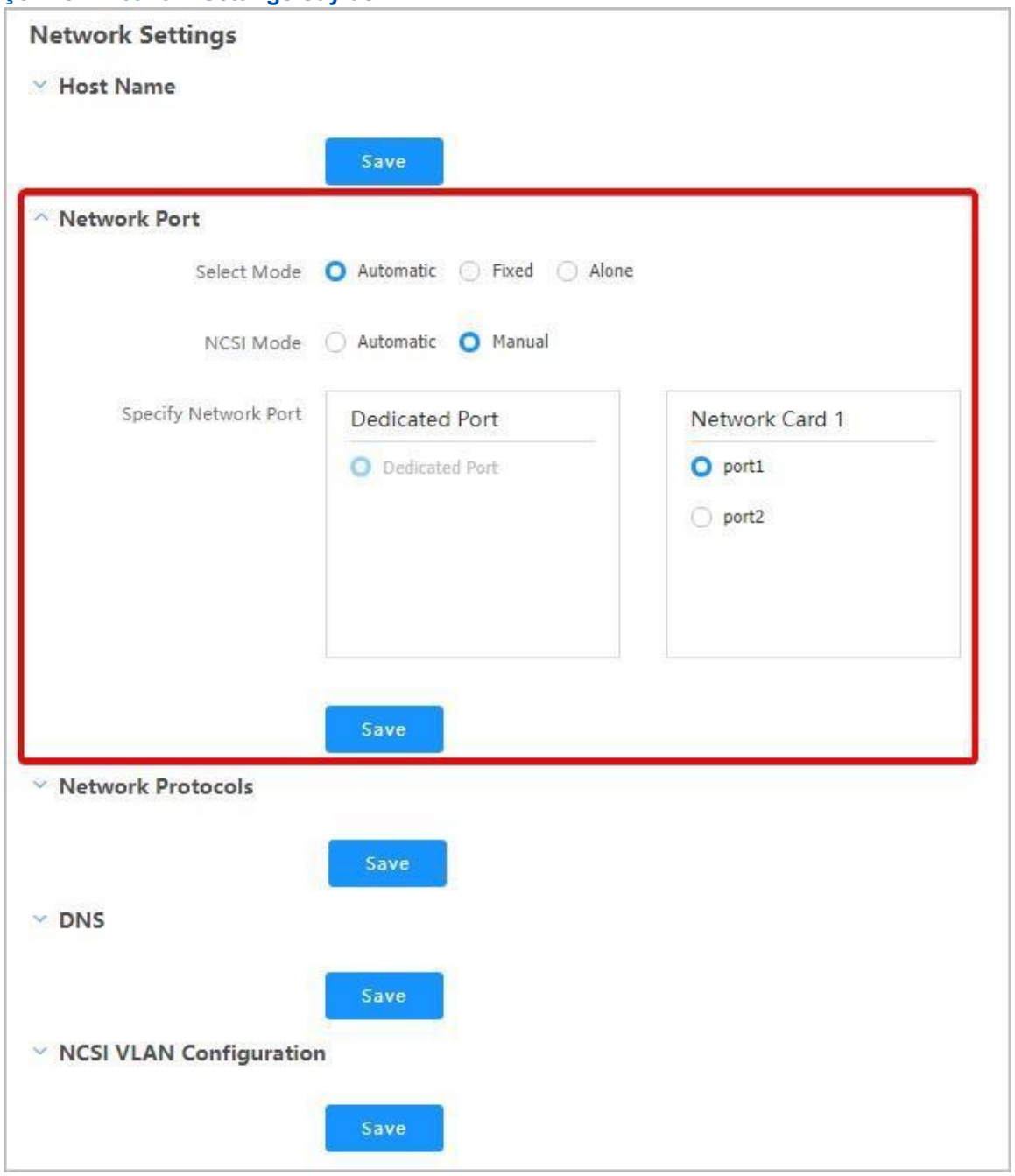
Özet

Bu prosedürde, yönetim ağ portunun ve paylaşılan ağ portunun belirlenmesi amacıyla ağ portu modunun nasıl yapılandırılacağı açıklanmıştır.

Adımlar

1. **BMC Settings'i** seçin. **BMC Settings** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Network Settings** seçimini yapın. **Network Settings** sayfası görüntülenir, bakınız Şekil 8-2.

Şekil 8-2 Network Settings Sayfası



3. **Network Port** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 8-2'ye başvurun.

Tablo 8-2 Network Port Modunun Yapılandırılması için Parametre Açıklamaları

Parametre	Ayarlar
Select Mode	Arzu edilen ağ portu modunu seçin. • **Automatic**: Özel ağ portu (yani iSAC ağ portu), tercihen yönetim ağ portu olarak kullanılır. Özel ağ portu düzgün bir şekilde çalışmıyorsa, özel ağ portunun yerine otomatik olarak düzgün çalışan bir yerleşik NCSI, yönetim ağ portu olarak kullanılır.

Parametre	Ayarlar
	. • **Fixed** : **Specify Network Port** alanındaki **Dedicated Port** kutusunda belirtilen bir ağ portu (özel ağ portu veya yerleşik NCSI), yönetim ağ portu olarak kullanılır. • **Alone**: Yönetim ağ portu ve paylaşılan ağ portu ayrı ayrı yapılandırılır. Yönetim ağ portu olarak bir özel (dedicated) ağ portu kullanılır ve yerleşik bir NCSI ise paylaşılan ağ portu olarak kullanılır. **Select Mode; Automatic** olarak ayarlandığında aşağıdaki parametrelerin yapılandırılmasına gerek yoktur.
NCSI Mode	**Alone** seçimi yapıldığında bu parametre gereklidir. Arzu edilen paylaşılan ağ portu modunu seçin. • **Automatic**: Paylaşılan ağ portu düzgün bir şekilde çalışmıyorsa, arızalı paylaşılan ağ portunun yerine otomatik olarak düzgün çalışan bir yerleşik **NCSI**, paylaşılan ağ portu olarak kullanılır. • **Manual**: **Specify Network Port** alanındaki **Network Card** kutusunda belirtilen bir yerleşik NCSI, paylaşılan ağ portu olarak kullanılır. Eğer **NCSI Mode** ; **Automatic** olarak ayarlandıysa herhangi bir paylaşılan ağ portunun belirtilmesine gerek yoktur.
Specify Network Port	• **Select Mode; Automatic** olarak ayarlandığında herhangi bir ağ portunun belirtilmesine gerek yoktur. • Eğer **Select Mode; Fixed** olarak ayarlandıysa, yönetim ağ portu olarak bir ağ portunun (özel ağ portu veya bir yerleşik NCSI) belirtilmesi gerekir. • Eğer **Select Mode; Alone** olarak ve **NCSI Mode; Manual** olarak ayarlandıysa, yönetim ağ portu olarak özel ağ portu kullanılır ve paylaşılan ağ portunun **Network Card** kutusunda bir yerleşik NCSI belirtilmesi gerekir.

4. **Save** üzerine tıklayın.

8.1.3 Ağ Portlarının IP Adreslerinin Yapılandırılması

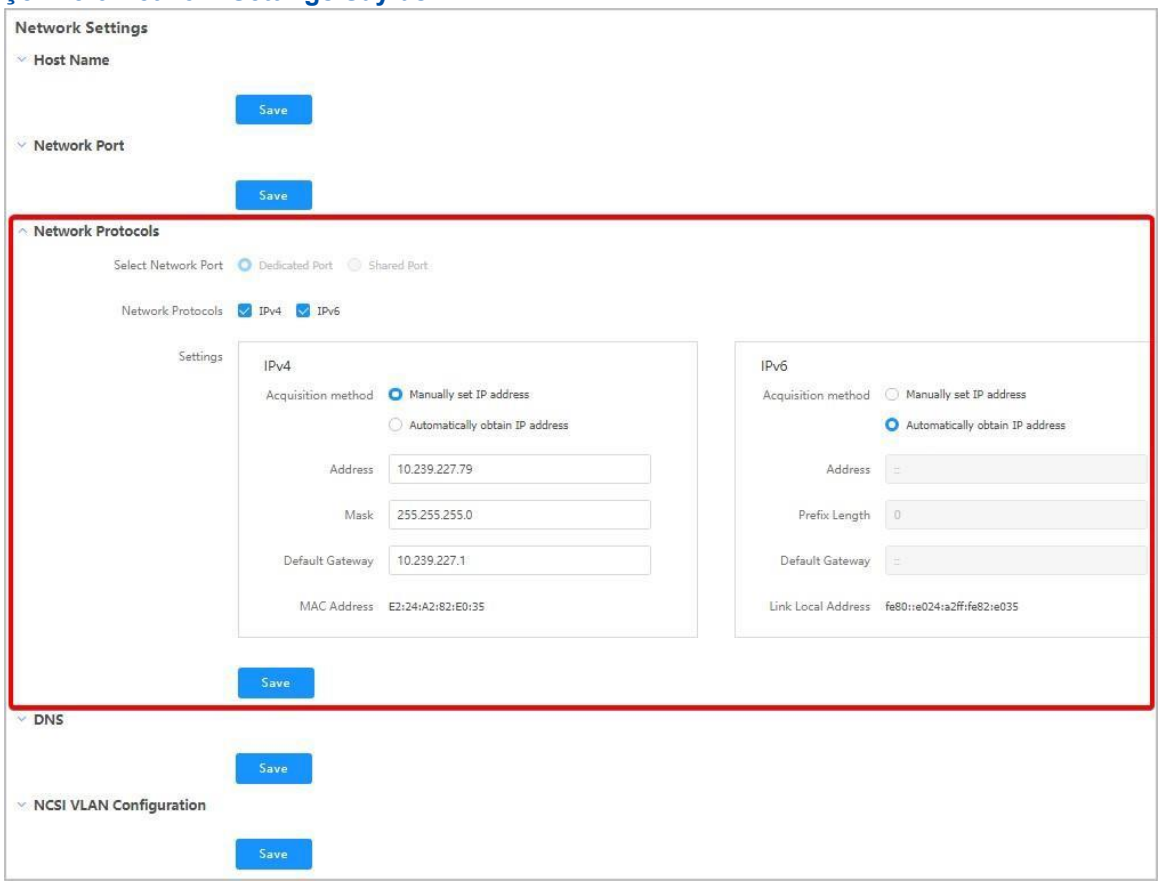
Özet

Sunucunun paylaşılan ağ portunun veya iSAC yönetim ağ portunun ağ IP adresinin yeniden planlanabilmesi için; IP adresi, alt-ağ maskesi, varsayılan ağ geçidi ve diğer ilgili bilgilerin yapılandırılması gereklidir.

Adımlar

1. **BMC Settings'i** seçin. **BMC Settings** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Network Settings** seçimini yapın. **Network Settings** sayfası görüntülenir, bakınız Şekil 8-3.

Şekil 8-3 Network Settings Sayfası



3. **Network Protocols** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 8-3'e başvurun.

Tablo 8-3 Network Protocol Parametre Açıklamaları

Parametre	Ayarlar
Select Network Port	Bu parametre sadece Network Port alanında **Select Mode**, **Alone** olarak ayarlandığında ayarlanabilir . Bir IP adresini yapılandırmak istediğiniz ağ portunu seçin. • **Dedicated Port**: iSAC yönetim ağ portunun IP adresini yapılandırır. • **Shared Port**: paylaşılan ağ portunun IP adresini yapılandırır.

Network Protocols	Ağ portu için ağ protokolünü(lerini) seçin. • Sadece **IPv4** seçmeniz durumunda IPv4 ayarlarının yapılandırılması gerekir. • Sadece **IPv6** seçmeniz durumunda IPv6 ayarlarının yapılandırılması gerekir. • **IPv4** ve **IPv6** seçmeniz durumunda hem IPv4 hem de IPv6 ayarlarının yapılandırılması gerekir.
Parametre	**Ayarlar**
Acquisition method	Bir IP adresi alma yöntemi seçin. **Acquisition method** değeri **Automatically obtain IP address** olarak ayarlandığında aşağıdaki parametrelerin yapılandırılması gerekmez.
Address	Planlandığı gibi BMC'nin IP adresini girin.
Mask	Maskeyi girin.
Default Gateway	Varsayılan Ağ Geçidi'nin IP adresini girin.

4. **Save** üzerine tıklayın.

8.1.4 DNS'nin Yapılandırılması

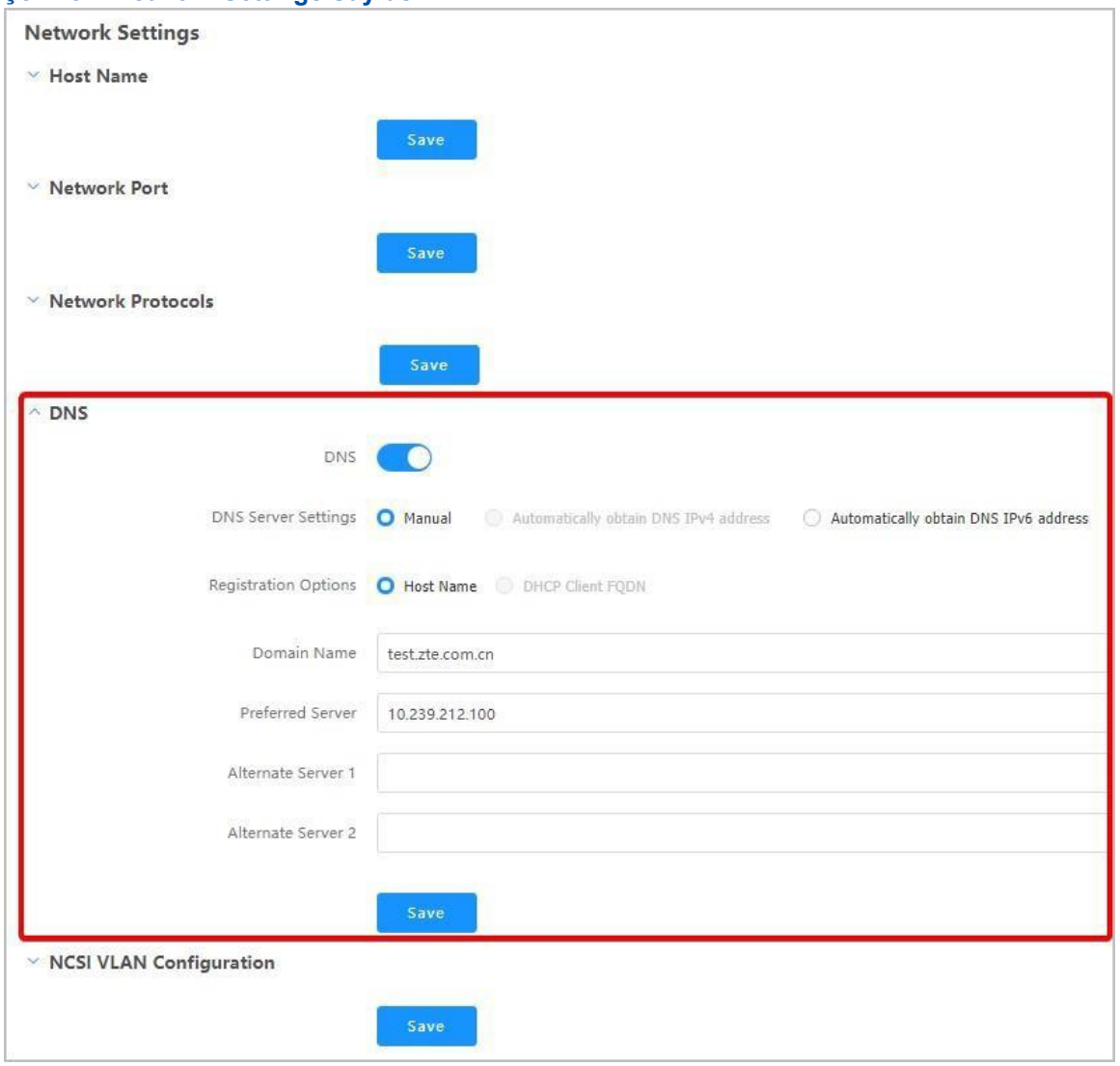
Özet

BMC'nin Web portalına bir FQDN üzerinden erişmek için sunucu hakkındaki DNS bilgisini yapılandırmanız gerekir.

Adımlar

1. **BMC Settings'i** seçin. **BMC Settings** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Network Settings** seçimini yapın. **Network Settings** sayfası görüntülenir, bakınız Şekil 8-4.

Şekil 8-4 Network Settings Sayfası



3. **DNS** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 8-4'e başvurun.

Tablo 8-4 DNS Parametre Açıklamaları

Parametre	Ayarlar
DNS	DNS hizmetini etkinleştirip etkinleştirmeyeceğinizi seçin. • DNS hizmetinin etkinleştirilmesi için **DNS** anahtarını açın. Bu durumda, aşağıdaki parametrelerin yapılandırılması gerekir. • DNS hizmetinin devre dışı bırakılması için **DNS** anahtarını kapatın. Bu durumda, aşağıdaki parametrelerin yapılandırılmasına gerek yoktur.
DNS Server Settings	Arzu edilen DNS ayarlama yöntemini seçin. • **Manual**: **Network Protocols** alanında **Acquisition method** değeri **Manually set IP address** olarak ayarlandıysa, bu parametrenin **Manual** olarak ayarlanması gerekir. **Manual** seçildiğinde aşağıdaki parametreleri yapılandırmanız gereklidir.

Parametre	Ayarlar
	• **Automatically obtain DNS IPv4 address**: Eğer **Network Protocols** alanında **Acquisition method** değeri **Automatically obtain IP address** ve **Network Protocols** değeri **IPv4** olarak ayarlandıysa, bu parametrenin **Automatically obtain DNS IPv4 address** olarak ayarlanması gereklidir. **Automatically obtain DNS IPv4 address** seçildiğinde, aşağıdaki parametreleri yapılandırmanıza gerek yoktur. • **Automatically obtain DNS IPv6 address**: Eğer **Network Protocols** alanında **Acquisition method** değeri **Automatically obtain IP address** ve **Network Protocols** değeri **IPv6** olarak ayarlandıysa, bu parametrenin **Automatically obtain DNS IPv6 address** olarak ayarlanması gereklidir. **Automatically obtain DNS IPv6 address** seçildiğinde, aşağıdaki parametreleri yapılandırmanıza gerek yoktur.
Registration Options	DNS'ye kayıt yaptırmak için kullanılacak seçeneği seçin. • **Host Name**: DNS'ye kaydolmak için DHCP option 12'yi kullanır. • **DHCP Client FQDN**: DNS'ye kayıt yaptırmak için DHCP option 81'i kullanır. Eğer DHCP sunucusu DHCP option 81'i desteklemiyorsa, **Host Name'i** seçin. Eğer **DNS Server Settings; Manual** olarak ayarlanırsa, sadece **Host Name** seçilebilir. Eğer **DNS Server Settings; Automatically obtain DNS IPv4 address** veya **Automatically obtain DNS IPv6 address** olarak ayarlanırsa, **Host Name** ya da **DHCP Client FQDN** seçilebilir.
Domain Name	Bir domain adı girin. Bir domain adı; rakamlar, harfler, kısa çizgiler (-) ve noktalar içerir ve en fazla 67 karakterden oluşur. Bir kısa çizgi ya da nokta ile başlayamaz veya bitemez. İki nokta arasında 63'den fazla karaktere izin verilmez
Preferred Server	Tercih edilen DNS sunucusunun IP adresini girin. **DNS Server Settings** değeri **Manual** olarak ayarlandıysa bu parametre gereklidir.
Alternate Server 1	Alternatif DNS sunucusu 1'in IP adresini girin. **DNS Server Settings** değeri **Manual** olarak ayarlandıysa bu parametre opsiyoneldir.
Alternate Server 2	Alternatif DNS sunucusu 2'nin IP adresini girin. **DNS Server Settings** değeri **Manual** olarak ayarlandıysa bu parametre opsiyoneldir.

4. **Save** üzerine tıklayın.

8.1.5 VLAN'ın Yapılandırılması

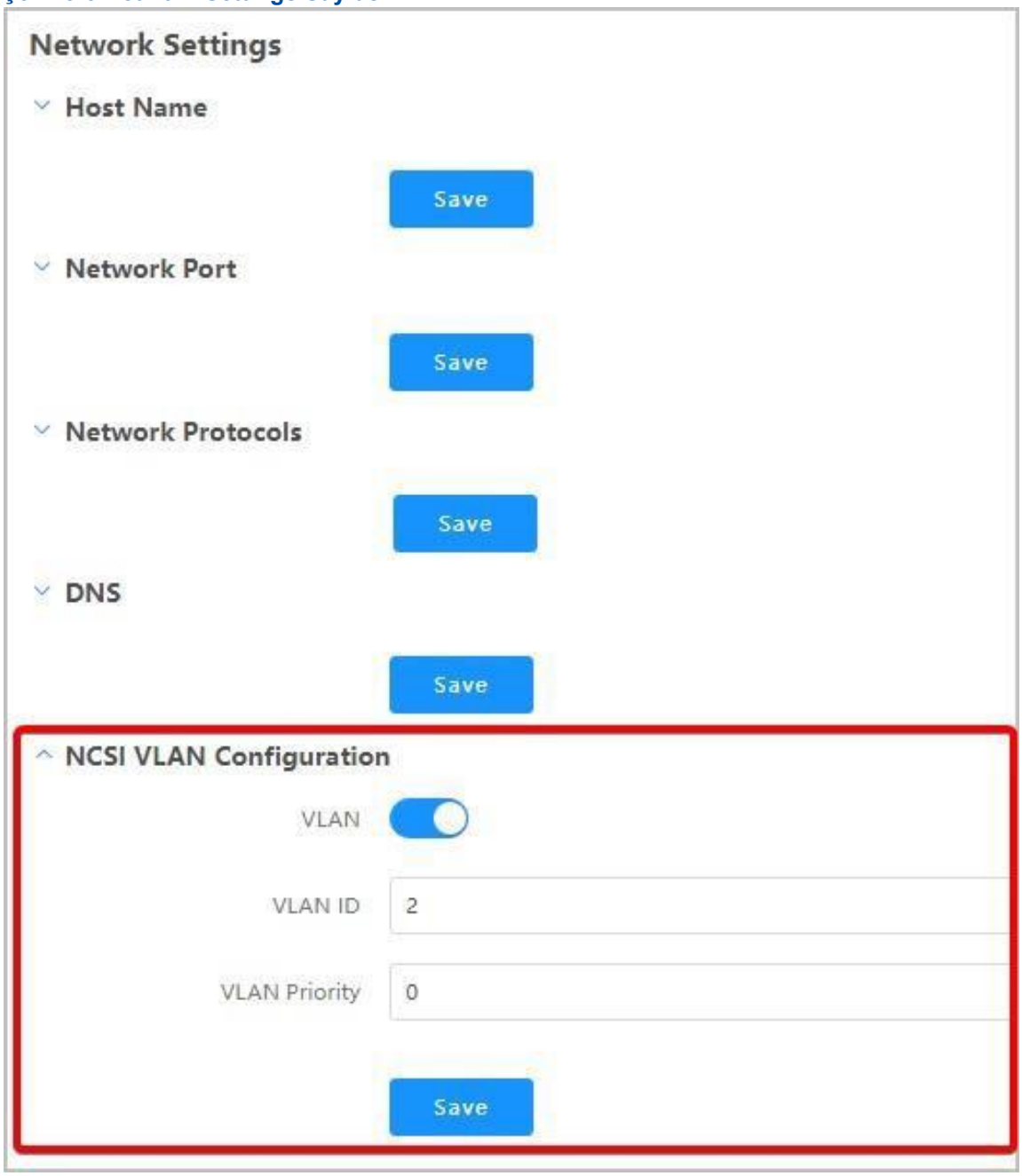
Özet

Bu prosedürde, yerleşik bir NCSI'nin VLAN'a eklenebilmesi için bir VLAN'ın nasıl yapılandırılacağı açıklanmıştır.

Adımlar

1. **BMC Settings'i** seçin. **BMC Settings** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Network Settings** seçimini yapın. **Network Settings** sayfası görüntülenir, bakınız Şekil 8-5.

Şekil 8-5 Network Settings Sayfası



3. **NCSI VLAN Configuration** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 8-5'e başvurun.

Tablo 8-5 NCSI VLAN Parametre Açıklamaları

Parametre	Ayarlar
VLAN	VLAN işlevinin etkinleştirilip etkinleştirilmeyeceğini seçin. • VLAN işlevinin etkinleştirilmesi için **VLAN** anahtarını açın. Bu durumda, aşağıdaki parametrelerin yapılandırılması gerekir. • VLAN işlevinin devre dışı bırakılması için **VLAN** anahtarını kapatın. Bu durumda, aşağıdaki parametrelerin yapılandırılmasına gerek yoktur. Aşağıdaki koşullardan herhangi birisi sağlanırsa, VLAN işlevi etkinleştirilebilir: • **Select Mode** parametresi **Network Port** alanında **Automatic** olarak ayarlanmıştır ve yerleşik bir NCSI bağlıdır. • **Select Mode** parametresi **Network Port** alanında **Fixed** olarak ayarlanmıştır ve yönetim ağ portu olarak yerleşik bir NCSI belirlenmiştir.
VLAN ID	VLAN Kimliğini girin. Aralık: 2–4094.
VLAN Priority	VLAN önceliğini girin. Aralık: 0–7. Daha büyük bir değer daha yüksek bir önceliği belirtir.

4. **Save** üzerine tıklayın.

8.2 Zaman Parametrelerinin Yapılandırılması

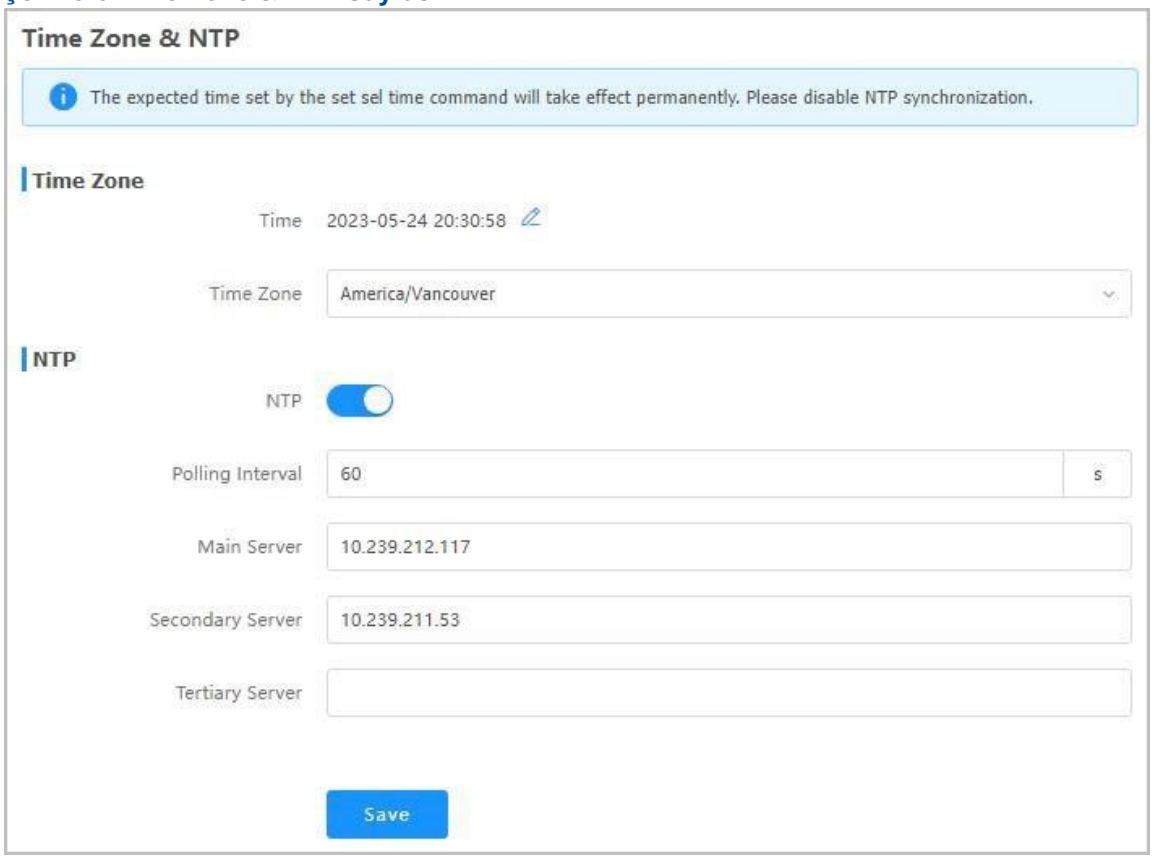
Özet

Bu prosedürde, BMC'nin doğru zaman bilgisini alabilmesi için zaman parametrelerinin nasıl yapılandırılacağı açıklanmıştır.

Adımlar

1. **BMC Settings'i** seçin. **BMC Settings** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Time Zone & NTP** seçimini yapın. **Time Zone & NTP** sayfası görüntülenecektir, bakınız Şekil 8-6.

Şekil 8-6 Time Zone & NTP Sayfası



3. Parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 8-6'ya başvurun.

Tablo 8-6 Time Configuration Parametre Açıklamaları

Parametre	Ayarlar
Time Zone	Saat dilimi gereken şekilde seçin.
NTP	NTP-tabanlı zaman sekronizasyonunun etkinleştirilip etkinleştirilmeyeceğine karar vermek için aşağıdakileri gerçekleştirin. • NTP-tabanlı zaman sekronizasyonunun etkinleştirilmesi için **NTP** anahtarını açın. • NTP-tabanlı zaman sekronizasyonunun devre dışı bırakılması için **NTP** anahtarını kapatın.
Polling Interval	Bu parametre, **NTP** anahtarı açıldığında gereklidir. Zaman senkronizasyonu süresini girin. Aralık: 60–65535, birim: saniye.
Main Server	Uzunluğu 127 karakteri aşmayacak şekilde birincil NTP sunucusunun FQDN veya IP adresini girin. Gereklidir.
Secondary Server	Uzunluğu 127 karakteri aşmayacak şekilde ikincil NTP sunucusunun FQDN veya IP adresini girin. Opsiyonel.
Tertiary Server	Uzunluğu 127 karakteri aşmayacak şekilde üçüncül NTP sunucusunun FQDN veya IP adresini girin. Opsiyonel.

Not

Eğer NTP-tabanlı zaman senkronizasyonu etkinleştirilmişse, BMC zamanı ilk olarak **Main Server** ile senkronize eder. Eğer senkronizasyon başarısız olursa, zamanı sırasıyla **Secondary Server** ve**Tertiary Server** ile senkronize eder.

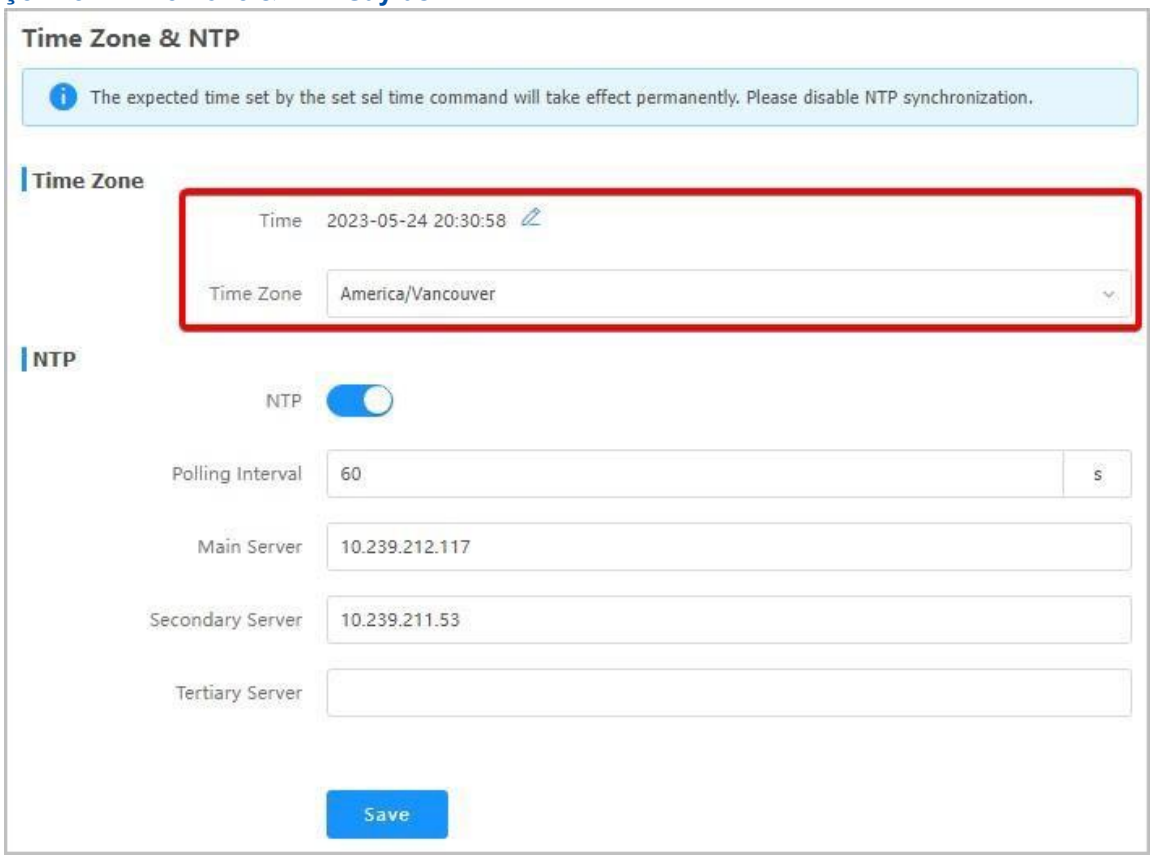
4. **Save** üzerine tıklayın.

Doğrulama

Eğer NTP-tabanlı zaman senkronizasyonu etkinleştirildiyse, doğrulama için aşağıdaki işlemleri gerçekleştirin:

1. **Time Zone & NTP** sayfasında, tarih ve saati kontrol edin, bakınız Şekil 8-7.

Şekil 8-7 Time Zone & NTP Sayfası



2. NTP sunucusunda, zaman bilgisinin BMC'ninki ile aynı olup olmadığını kontrol edin.

8.3 BMC'nin Web Portalında BMC'nin Sıfırlanması

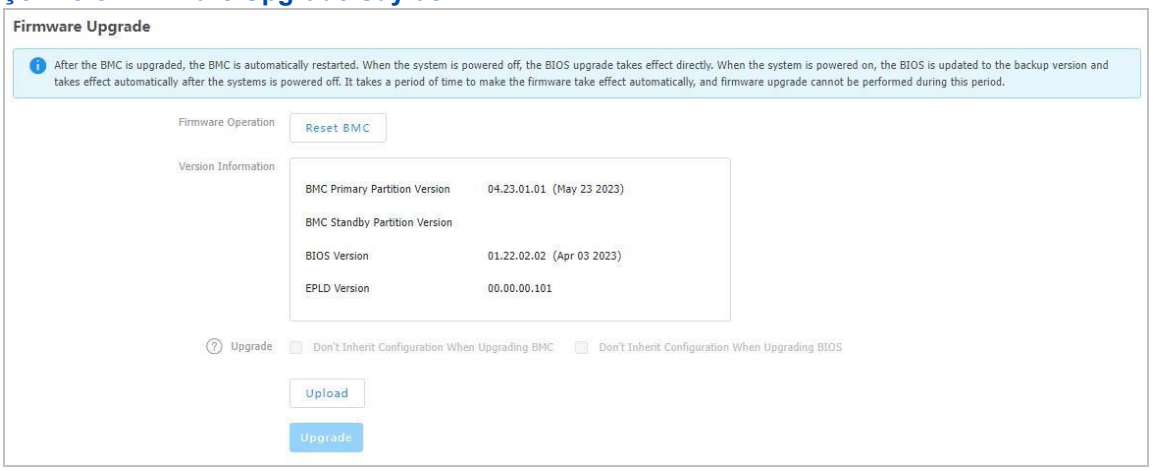
Özet

Bazı yapılandırmalardan sonra (örneğin; MAC adresi ve şasi bilgisi programlama), değişiklikleri uygulamak için BMC'yi sıfırlamanız gerekir.

Adımlar

1. **BMC Settings'i** seçin. **BMC Settings** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Firmware Upgrade** seçimini yapın. **Firmware Upgrade** sayfası görüntülenir, bakınız Şekil 8-8.

Şekil 8-8 Firmware Upgrade Sayfası



3. **Reset BMC** üzerine tıklayın ve görüntülenen mesaj kutusunda sıfırlama işlemini onaylayın.

Not

Yeniden oturum açılmasına sadece BMC sıfırlandıktan sonra izin verilir.

8.4 Firmware'ın Yükseltilmesi

Özet

Eğer sunucunun ana kartındaki firmware'nin yükseltilmesi gerekliyse, firmware yükseltme işlemini gerçekleştirmek için firmware'yi çevrimiçi olarak yükleyebilirsiniz.
Eğer birden fazla firmware sürümünün yükseltilmesi gerekliyse aşağıdaki sıralamanın uygulanması önerilir:

1. EPLD firmware
   EPLD firmware yükseltildikten sonra, yeni sürüm ancak sunucu yeniden başlatıldıktan sonra yürürlüğe girer. Bu nedenle yükseltme işlemini gerçekleştirmeden önce sunucuda koşan hizmetleri durdurmanız önerilir.
2. BMC firmware
   BMC firmware yükseltildikten sonra yükseltilen sürümün uygulanması için BMC otomatik olarak yeniden başlatılır.
3. BIOS firmware

- Eğer BIOS firmware, sunucu kapalıyken yükseltilirse, yükseltilen BIOS firmware doğrudan yürürlüğe girer.
- Eğer BIOS firmware, sunucu açıkken yükseltilirse, yükseltilen BIOS firmware Web portalda yedek bir sürüm olarak görüntülenir ve sunucu kapatıldıktan sonra otomatik olarak yürürlüğe girer. Sistem geçerli yükseltme sürümünü otomatik olarak uygularken başka hiçbir firmware yükseltme işlemi gerçekleştirilemez.

Not

Sürüm yükseltme sırasında bir firmware sürümü yükseltilemezse, bu firmware sürümünü yeniden yükseltmeniz gerekir.

Önkoşul

Yükseltilecek olan firmware halihazırda alınmış olmalıdır.

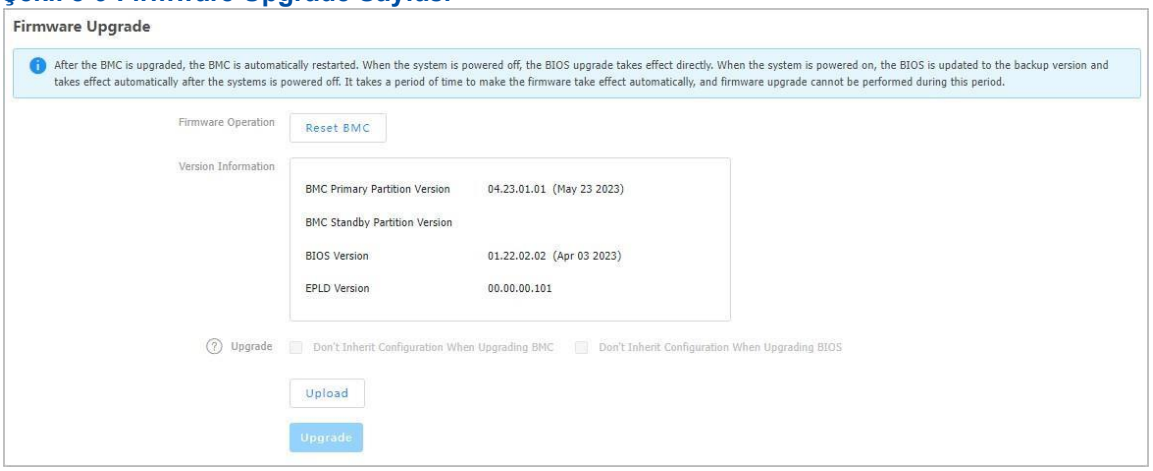
Not

Firmware dosyaları, sunucu ve depolama ürünlerinin Web portalındaki **Software Download** sayfasından edinilebilir (https://destek.netas.com.tr).

Adımlar

1. **BMC Settings'i** seçin. **BMC Settings** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Firmware Upgrade** seçimini yapın. **Firmware Upgrade** sayfası görüntülenir, bakınız Şekil 8-9.

Şekil 8-9 Firmware Upgrade Sayfası



3. **Upload** üzerine tıklayın ve görüntülenen iletişim kutusunda firmware dosyasını seçin.

Not

Bir seferde sadece tek bir firmware dosyası seçilebilir. Firmware yükseltme işlemi esnasında, firmware dosyası otomatik olarak firmware türüyle eşleşir.

4. **Upgrade** üzerine tıklayın.

Uyarı

Firmware yükseltme işlemi esnasında başka bir sayfaya geçemezsiniz. Aksi taktirde yükseltme işlemi kesintiye uğrar.

8.5 BMC Konfigürasyonlarının Güncellenmesi

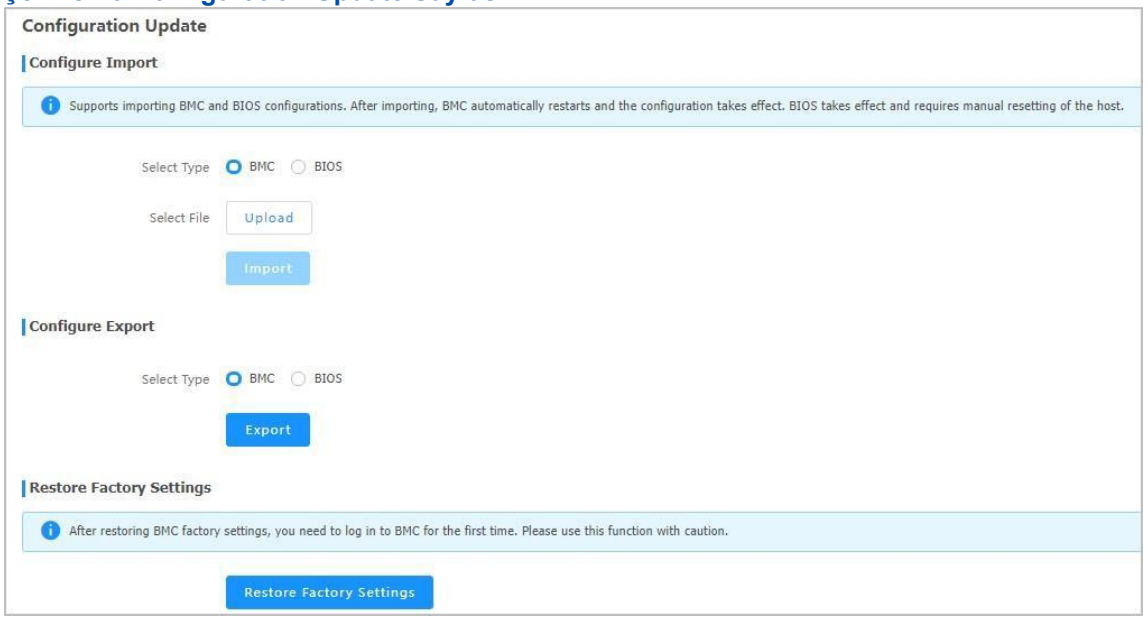
Özet

Bu prosedürde, BMC konfigürasyonlarının çevrimiçi olarak nasıl güncelleneceği açıklanmıştır. Bir sunucunun ana kartını değiştirmeden önce, BMC konfigürasyon güncelleme işlevini kullanarak BMC'nin konfigürasyonlarını yedekleyebilirsiniz.

Adımlar

1. **BMC Settings'i** seçin. **BMC Settings** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Configuration Update** seçimini yapın. **Configuration Update** sayfası görüntülenecektir, bakınız Şekil 8-10.

Şekil 8-10 Configuration Update Sayfası



3. Aşağıdaki işlemleri gerektiği gibi gerçekleştirin.

Eğer…	O zaman aşağıda belirtilenleri yapmanız gerekmektedir

Eğer mevcut bir BMC yapılandırma dosyası varsa;	a. **Upload** üzerine tıklayın ve görüntülenen iletişim kutusunda BMC yapılandırma dosyasını seçin. b. **Import**'a tıklayın ve görüntülenen ileti kutusunda içeri aktarma işlemini onaylayın.
Eğer BMC yapılandırma dosyası yoksa;	a. Geçerli BMC konfigürasyonlarını yerel PC'nize aktarmak için **Export** üzerine tıklayın. b. Dışarı aktarılan BMC yapılandırma dosyasını düzenleyin. c. **Upload** üzerine tıklayın ve görüntülenen iletişim kutusunda BMC yapılandırma dosyasını seçin. d. **Import**'a tıklayın ve görüntülenen ileti kutusunda içeri aktarma işlemini onaylayın.

Not

BMC konfigürasyonları içeri aktarıldıktan sonra konfigürasyonların uygulanması için BMC otomatik olarak yeniden başlatılır. BMC yeniden başlatılana kadar hiçbir işlem gerçekleştirmeyin.

İlgili Görevler

BMC konfigürasyonlarını yedeklemek için aşağıdaki işlemleri gerçekleştirin:

1. Geçerli BMC konfigürasyonlarını yerel PC'nize aktarmak için **Export** üzerine tıklayın.
2. Ana kartı değiştirdikten sonra **Upload** üzerine tıklayın ve görüntülenen iletişim kutusu içerisinde dışarı aktarılmış olan BMC konfigürasyonunu seçin.
3. **Import**'a tıklayın ve görüntülenen ileti kutusunda içeri aktarma işlemini onaylayın.

8.6 Varsayılan Fabrika Ayarlarını Geri Yükleme

Özet

Varsayılan fabrika ayarlarını geri yükleyerek, sunucu yapılandırma öğelerini (örneğin; ağ, kullanıcı, SNMP konfigürasyonu ve başlatma modu) fabrika ayarlarına döndürebilirsiniz.

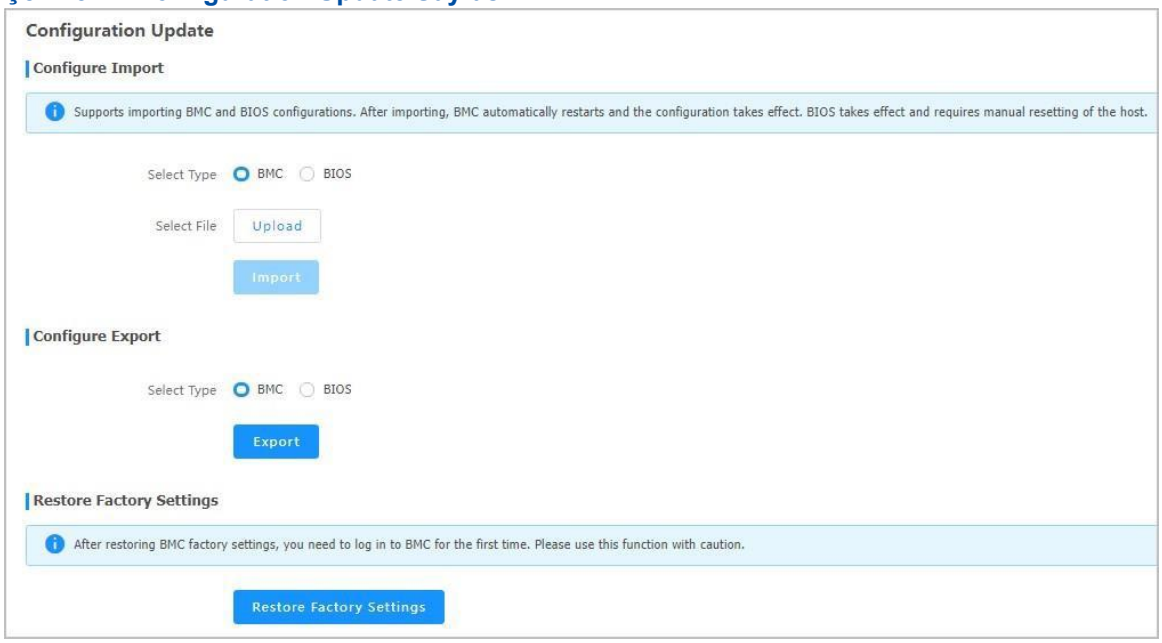
Not

Geri yükleme esnasında herhangi bir işlem gerçekleştirmeyin.
Varsayılan fabrika ayarları geri yüklendikten sonra, BMC otomatik olarak yeniden başlatılacaktır.

Adımlar

1. **BMC Settings'i** seçin. **BMC Settings** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Configuration Update** seçimini yapın. **Configuration Update** sayfası görüntülenecektir, bakınız Şekil 8-11.

Şekil 8-11 Configuration Update Sayfası



3. **Restore Factory Defaults** üzerine tıklayın.

Bölüm 9
Kullanıcı ve Güvenlik

İçindekiler Tablosu

9.1 Bir Yerel Kullanıcının Eklenmesi

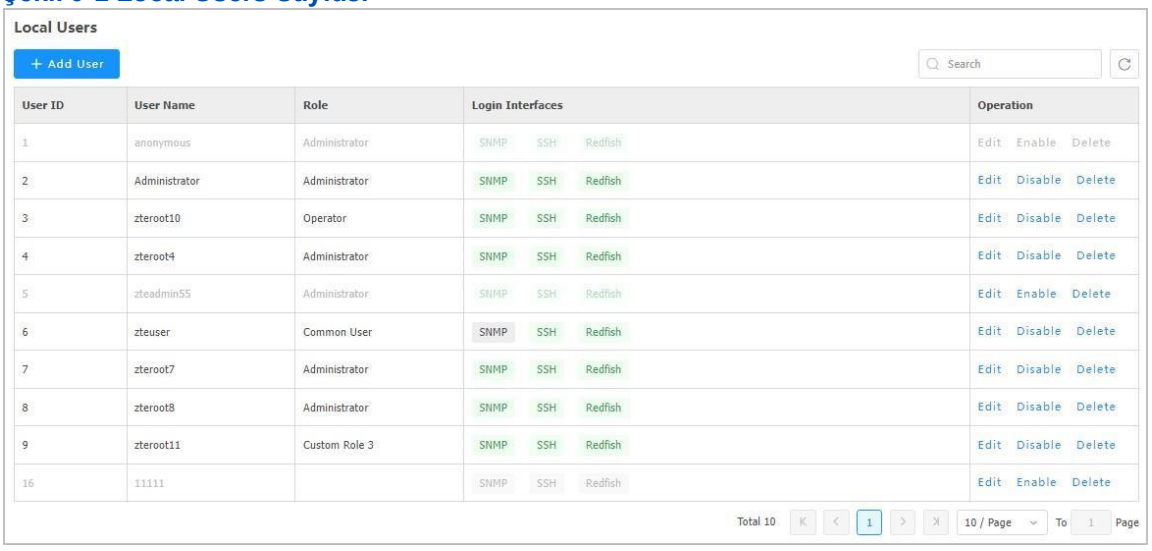
Özet

Yerel kullanıcılar, BMC'nin kendi kullanıcılarını ifade eder. Bu prosedürde, BMC'nin yapılandırılması ve yönetilmesi için bir yerel kullanıcının nasıl ekleneceği açıklanmıştır.

Adımlar

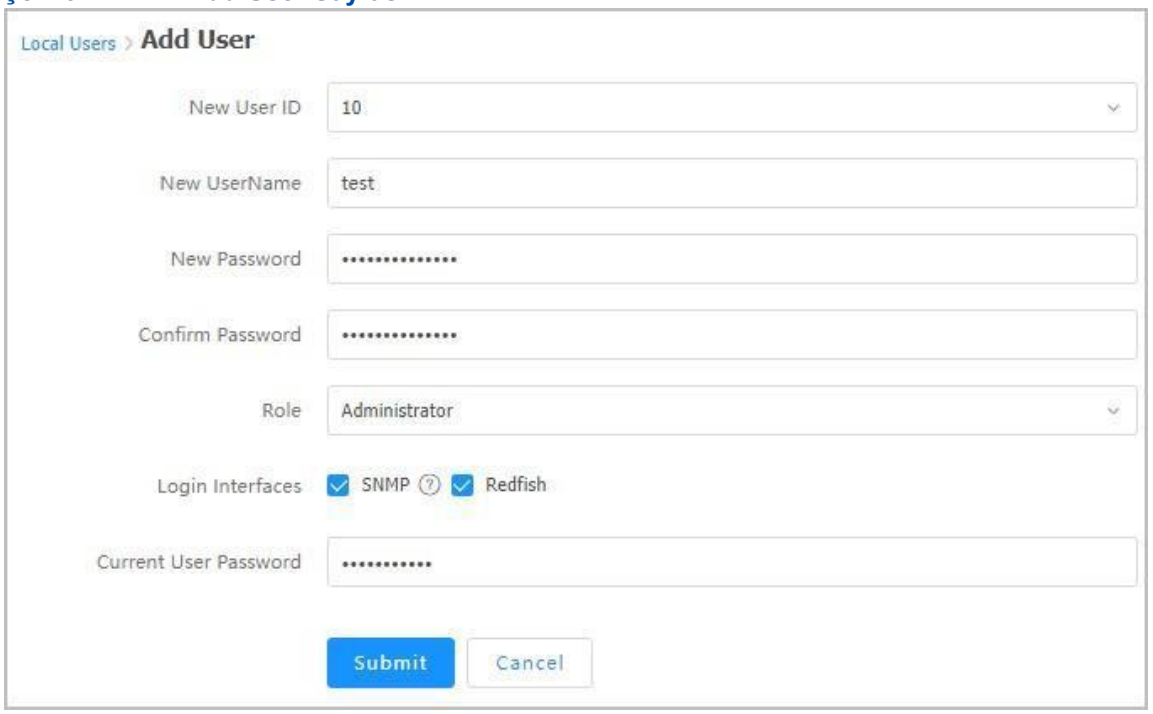
1. **User & Security** seçimini yapın. **User& Security** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Local Users** seçimini yapın. **Local Users** sayfası görüntülenir, bakınız Şekil 9-1.

Şekil 9-1 Local Users Sayfası



3. **Add User** üzerine tıklayın. **Add User** sayfası görüntülenir, bakınız Şekil 9-2.

Şekil9-2 Add User Sayfası



4. Parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 9-1'e başvurun.

Tablo 9-1 Bir Yerel Kullanıcı Eklemeye Dair Parametre Açıklamaları

Parametre	Ayarlar
New User ID	Yeni kullanıcının ID'sini seçin. En fazla 16 yerel kullanıcı desteklenir, bu nedenle user ID değeri 1 ila 16 arasında bir değerdir. Kullanıcı 1 ayrılmış bir kullanıcı olup Kullanıcı 2 ise varsayılan sistem yöneticisidir.
New UserName	Yeni kullanıcının adını girin. Bu ad; rakamlar, harfler (büyük/küçük harfe duyarlı) ve özel karakterler içerir ve en fazla 16 karakterden oluşur. Yeni kullanıcı adı (username) başka bir mevcut kullanıcı adı ile aynı olamaz. Şunlar kullanıcı adı olarak kullanılamaz: sshd, ntp, stunnel4, sysadmin, daemon, Administrator ve anonymous
New Password	Yeni kullanıcının parolasını girin. Bu parola; rakamlar, harfler (büyük/küçük harfe duyarlı) ve özel karakterler içerir ve 5 ila 20 karakterden oluşur. Eski parolalar yeniden kullanılamaz.
Confirm Password	Doğrulama için aynı parolayı tekrar girin.
Role	Yeni kullanıcının rolünü seçin.
Login Interfaces	Yeni kullanıcı için kullanılabilir olan bir veya daha fazla oturum açma arayüzü seçin. • SNMP arayüzü tabanlı oturum açma için **SNMP**'yi seçin.

Parametre	Ayarlar
	• Redfish arayüzü tabanlı oturum açma için **Redfish**'i seçin. SSH tabanlı oturum açma varsayılan olarak tüm kullanıcılar için desteklenir.
Current User Password	Mevcut durumda oturum açmış olan kullanıcının parolasını girin.

5. **Submit** üzerine tıklayın.
6. (Opsiyonel) Eğer **Login Interfaces** değeri **SNMP** olarak ayarlandıysa, yeni kullanıcı için **Operation** sütununda **Edit** üzerine tıklayın. **Edit** sayfası görüntülenir. **SNMPv3 Authentication Algorithm** ve **SNMPv3 Encryption Algorithm** değerlerini ayarlayın.

İlgili Görevler

Aşağıdaki işlemlerden birini gerektiği gibi gerçekleştirin.

Aşağıdakileri gerçekleştirmek için...	Şunları yapın...
Bir yerel kullanıcının devre dışı bırakılması	1. **Operation** sütununda kullanıcı için **Disable** üzerine tıklayın. **Confirm** iletişim kutusu görüntülenir. 2. Mevcut durumda oturum açmış olan kullanıcının parolasını girin. 3. **Submit** üzerine tıklayın.
Bir yerel kullanıcının silinmesi	1. **Operation** sütununda kullanıcı için **Delete** üzerine tıklayın. **Confirm** iletişim kutusu görüntülenir. 2. Mevcut durumda oturum açmış olan kullanıcının parolasını girin. 3. **Submit** üzerine tıklayın.

9.2 Domain Kullanıcıları için Kimlik Doğrulama Parametrelerinin Yapılandırılması.

Özet

Domain kullanıcıları, BMC'nin kendi kullanıcıları değildir. Domain kullanıcıları ile ilgili ayrıntılı bilgiler bir LDAP sunucusunda veya AD sunucusunda saklanır.
Bu prosedürde, domain kullanıcılarının bir LDAP veya AD sunucusu üzerinden kimlik doğrulamasına tabi tutulması için kimlik doğrulama parametrelerinin nasıl yapılandırılacağı açıklanmıştır.

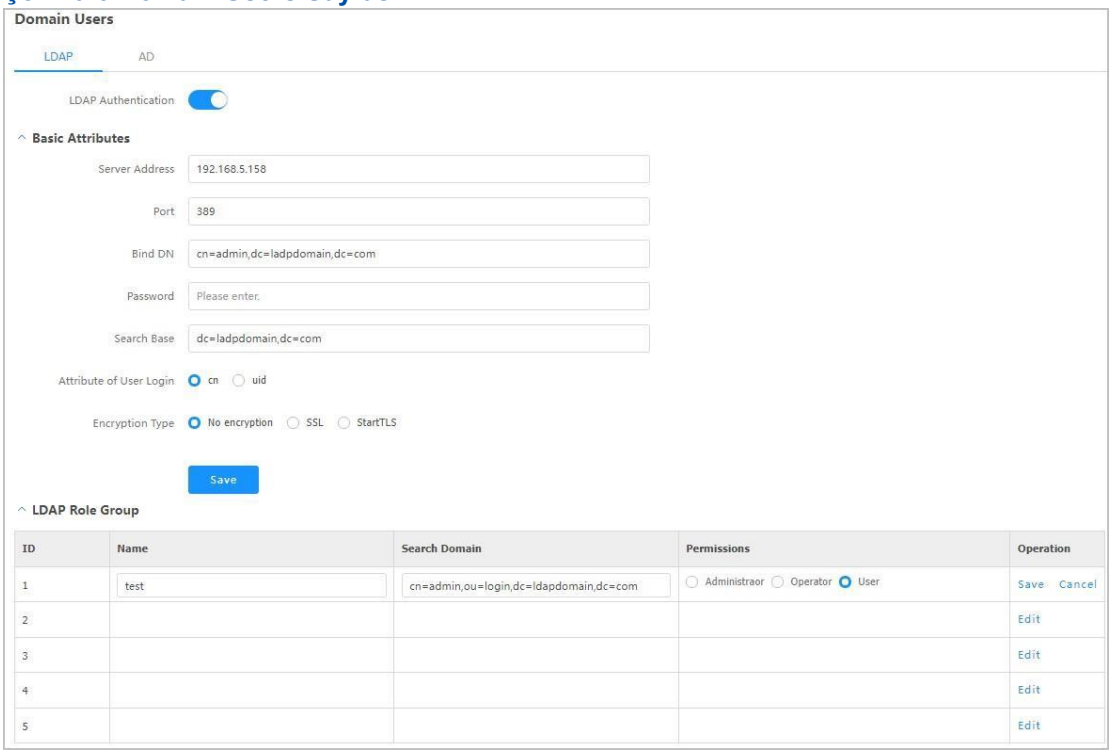
Önkoşul

LDAP sunucusu veya AD sunucusunun parametreleri halihazırda alınmış olmalıdır.

Adımlar

- LDAP Server Authentication Parametrelerinin Yapılandırılması
  1. **User & Security** seçimini yapın. **User& Security** sayfası görüntülenir.
  2. Sol taraftaki navigasyon ağacından, **Domain Users** seçimini yapın. **Domain Users** sayfası görüntülenir, bakınız Şekil 9-3.

Şekil 9-3 Domain Users Sayfası



3. **LDAP Authentication** anahtarını açın.
4. **Basic Attributes** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 9-2'ye başvurun.

Tablo 9-2 Basic LDAP Authentication Attributes için Parametre Açıklamaları

Parametre	Ayarlar
Server Address	LDAP sunucusunun FQDN veya IP adresini girin.
Port	Port numarasını girin. Aralık: 1–65535. Varsayılan: 389. Eğer **Encryption Type; SSL** olarak ayarlandıysa, port numarası olarak *636* girin.
Bind DN	LDAP sunucusunun DN'sini girin; örneğin, *cn=admin,dc=ldapdomain,dc=com*.
Password	LDAP sunucusunda oturum açmak için parolayı girin. Bu alan boş bırakılamaz. Aralık: 1-47 karakter. LDAP sunucusuna erişmek için **Bind DN** ve **Password** kullanılır.
Search Base	LDAP sunucusunda kullanıcı bilgisinin saklanacağı lokasyonu girin, örneğin; *dc=ldapdomain,dc=com*.
Attribute of User Login	LDAP sunucusu tarafından tanımlanan kullanıcı oturum açma niteliklerini seçin. → Eğer **Bind DN,** cn içeriyorsa **cn** seçin. → Eğer **Bind DN,** uid içeriyorsa **uid** seçin.

Encryption Type	LDAP sunucusu tarafından kullanılan şifreleme türünü seçin. → **No encryption**: şifreleme kullanılmadığını belirtir.
Parametre	**Ayarlar**
	→ **SSL**: SSL şifrelemenin kullanıldığını belirtir. → **StartTLS**: StartTLS şifreleme kullanıldığını belirtir.
Upload certificate	İlgili sertifika butonuna tıklayın ve sertifikayı yükleyin. Eğer **Encryption Type** değeri **No encryption** olarak ayarlandıysa, sertifika yüklenmesine gerek yoktur.

5. **Save** üzerine tıklayın.
6. Rol grup parametrelerini etkinleştirmek için **LDAP Role Group** alanında, **Operation** kolonunda bir rol grubu için **Edit** üzerine tıklayın.
7. Role group parametrelerini ayarlayın. Parametrelerin açıklamaları için, Tablo 9-3'e başvurun.

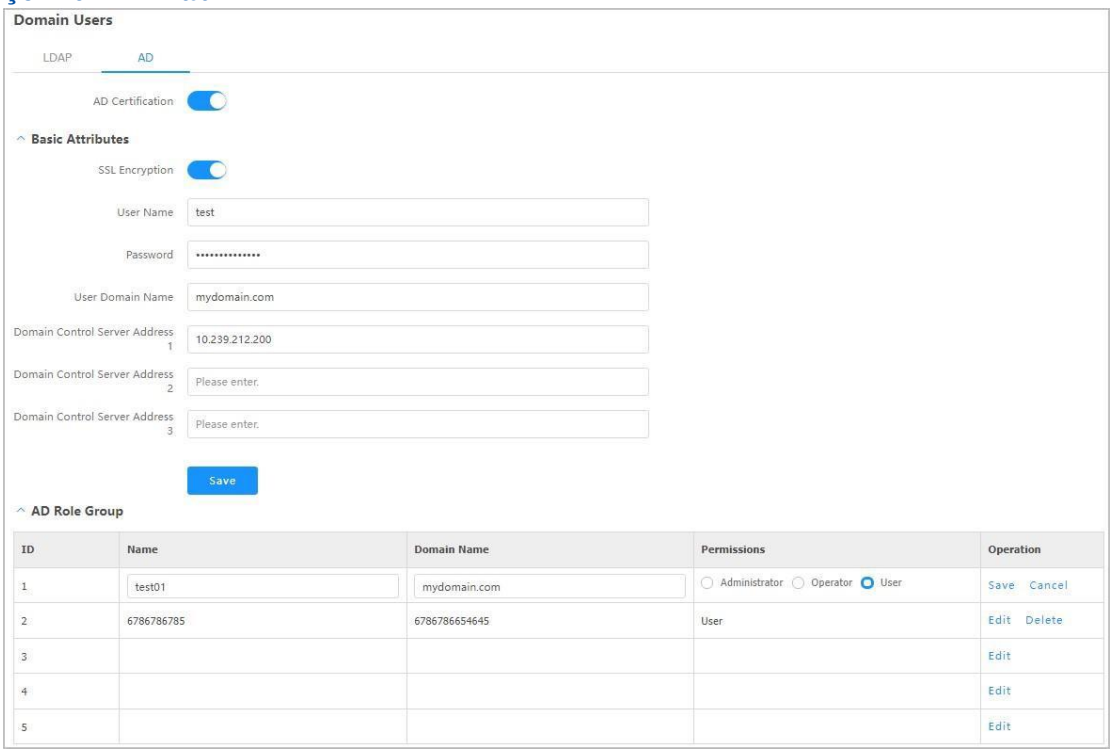
Tablo 9-3 LDAP Role Group Parametre Açıklamaları

Parametre	**Ayarlar**
Name	Domain kullanıcısının ait olduğu rol grubunu girin. Bu ad; rakamlar, harfler, boşluklar ve özel karakterler içerir ve en fazla 64 karakterden oluşur. Boşluk ile başlayamaz. İzin verilen özel karakterler, kısa çizgileri (-) ve alt çizgileri (_) içerir.
Search Domain	LDAP sunucusunda kullanıcı grubu bilgisinin saklanacağı lokasyonu girin, örneğin; `cn=admin,ou=login,dc=ldapdomain,dc=com`.
Permissions	BMC'de rol grubunun işlem izinlerini seçin.

8. **Operation** sütununda **Save** üzerine tıklayın.

- AD Server Authentication Parametrelerinin Yapılandırılması
  1. **User & Security** seçimini yapın. **User& Security** sayfası görüntülenir.
  2. Sol taraftaki navigasyon ağacından, **Domain Users** seçimini yapın. **Domain Users** sayfası görüntülenir.
  3. **AD** üzerine tıklayın. **AD** sekmesi görüntülenir, bakınız Şekil 9-4.

Şekil 9-4 AD Tab



4. **AD Authentication** anahtarını açın.
5. **Basic Attributes** alanındaki parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 9-4'e başvurun.

Tablo 9-4 Basic AD Authentication Attributes için Parametre Açıklamaları

Parametre	Ayarlar
SSL Encryption	AD sunucusunda oturum açarken SSL şifrelemenin kullanılıp kullanılmayacağına arar vermek için aşağıdakileri gerçekleştirin. → SSL şifrelemeyi etkinleştirmek için **SSL Encryption** anahtarını açın. → SSL şifrelemeyi devre dışı bırakmak için **SSL Encryption** anahtarını kapatın.
User Name	AD sunucusunda oturum açmak için kullanıcı adını girin. Bu kullanıcı adı; rakamlar, harfler (büyük/küçük harfe duyarlı), boşluklar ve özel karakterler içerir ve en fazla 64 karakterden oluşur. Bir harf ile başlamalıdır. İzin verilen özel karakterler, kısa çizgileri (-) ve alt çizgileri (_) içerir. Eğer kullanıcı adı ve parola gerekli değilse, bu parametreyi boş bırakın.
Password	AD sunucusunda oturum açmak için parolayı girin. Aralık: 6-127 karakter. Eğer kullanıcı adı ve parola gerekli değilse, bu parametreyi boş bırakın.

User Domain Name	AD sunucusunun domain adını girin; örneğin; *mydomain.com*. Gereklidir.
Parametre	**Ayarlar**
Domain Control Server Address 1	IPv4 ve Ipv6 formatlarını destekleyen AD sunucusu 1'in IP adresini girin. Gereklidir.
Domain Control Server Address 2	IPv4 ve Ipv6 formatlarını destekleyen AD sunucusu 2'nin IP adresini girin. Opsiyoneldir.
Domain Control Server Address 3	IPv4 ve Ipv6 formatlarını destekleyen AD sunucusu 3'ün IP adresini girin. Opsiyoneldir.

6. **Save** üzerine tıklayın.
7. Rol grup parametrelerini etkinleştirmek için **AD Role Group** alanında, **Operation** kolonunda bir rol grubu için **Edit** üzerine tıklayın.
8. Role group parametrelerini ayarlayın. Parametrelerin açıklamaları için, Tablo 9-5'e başvurun.

Tablo 9-5 AD Role Group Parametre Açıklamaları

Parametre	Ayarlar
Name	Domain kullanıcısının ait olduğu rol grubunu girin. Bu ad; rakamlar, harfler, boşluklar ve özel karakterler içerir ve en fazla 64 karakterden oluşur. Boşluk ile başlayamaz. İzin verilen özel karakterler, kısa çizgileri (-) ve alt çizgileri (_) içerir.
Domain Name	Rol grubunun domain adını girin, örneğin; *mydomain.com*.
Permissions	BMC'de rol grubunun işlem izinlerini seçin.

9. **Operation** sütununda **Save** üzerine tıklayın.

9.3 Çevrimiçi Kullanıcıların Sorgulanması

Özet

Çevrimiçi kullanıcıları sorgulayarak, tüm çevrimiçi kullanıcılar hakkında ID'leri, kullanıcı adları, oturum açma modları, oturum açma IP adresleri ve oturum açma zamanları gibi bilgileri öğrenebilirsiniz.

Not

Bu ID, user ID yerine kullanıcının bağlantı oturumunun seri numarasıdır.

Adımlar

1. **User & Security** seçimini yapın. **User& Security** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Online Users** seçimini yapın. **Online Users** sayfası görüntülenir, bakınız Şekil 9-5.

Şekil 9-5 Online Users Sayfası

3. (Opsiyonel) Bir kullanıcıyı BMC'nin Web portalındaki oturumunu kapatmaya zorlamak için, o kullanıcı için **Operation** sütununda **Delete** üzerine tıklayın ve görüntülenen iletişim kutusunda **Submit** üzerine tıklayın.

9.4 İsteğe Uyarlanmış Bir Rol için İzinlerin Yapılandırılması

Özet

Aşağıdaki roller sistemde varsayılan olarak mevcuttur:

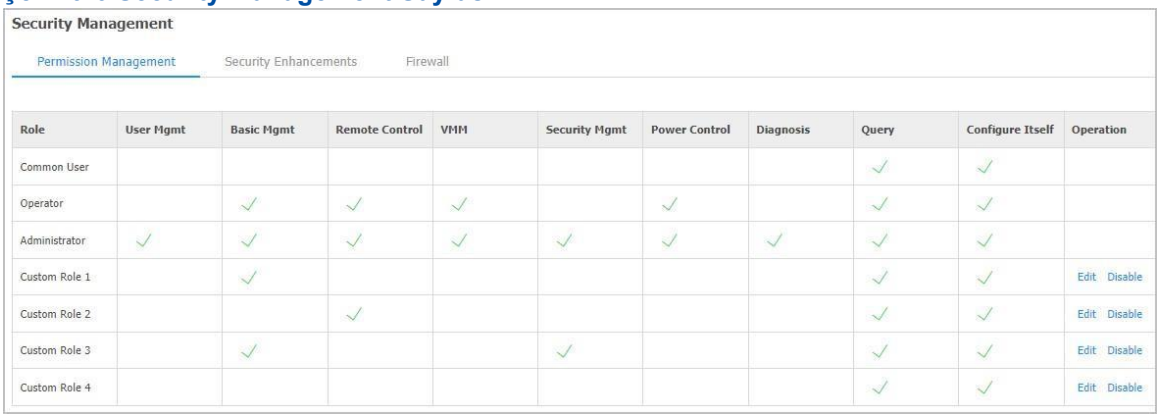
- Genel kullanıcı
- Operatör
- Sistem Yöneticisi (Admin)
- İsteğe uyarlanmış roller 1–4

Genel kullanıcıların, operatörlerin ve sistem yöneticilerinin izinleri yapılandırılamaz ancak isteğe uyarlanmış rollerin izinleri yapılandırılabilir.

Adımlar

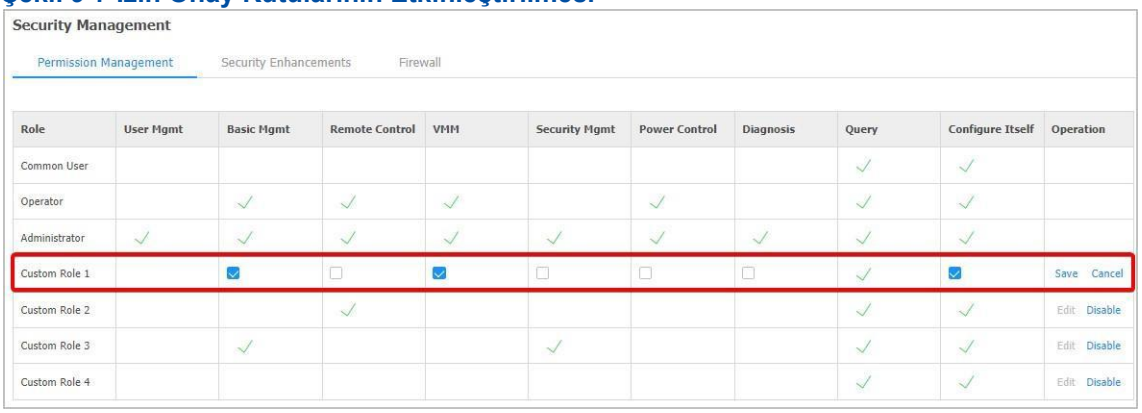
1. **User & Security** seçimini yapın. **User& Security** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Security Management** seçimini yapın. **Security Management** sayfası görüntülenir, bakınız Şekil 9-6.

Şekil 9-6 Security Management Sayfası



3. **Operation** sütununda, izin onay kutularını etkinleştirmek amacıyla isteğe uyarlanmış bir rol için **Edit** üzerine tıklayın, bakınız Şekil 9-7.

Şekil 9-7 İzin Onay Kutularının Etkinleştirilmesi



4. İlgili izinleri seçin.
5. **Save** üzerine tıklayın.

İlgili Görevler

İsteğe uyarlanmıi bir rolü devre dışı bırakmak veya etkinleştirmek için aşağıdaki işlemleri gerçekleştirin:

- İsteğe uyarlanan rolü devre dışı bırakmak için **Operation** sütununda **Disable** üzerine tıklayın.

Not

Genel kullanıcıları, operatörleri ve sistem yöneticilerini devre dışı bırakamaz veya etkinleştiremezsiniz.

- İsteğe uyarlanan rolü etkinleştirmek için **Operation** sütununda **Enable** üzerine tıklayın.

9.5 Güvenlik Geliştirme Parametrelerinin Yapılandırılması

Özet

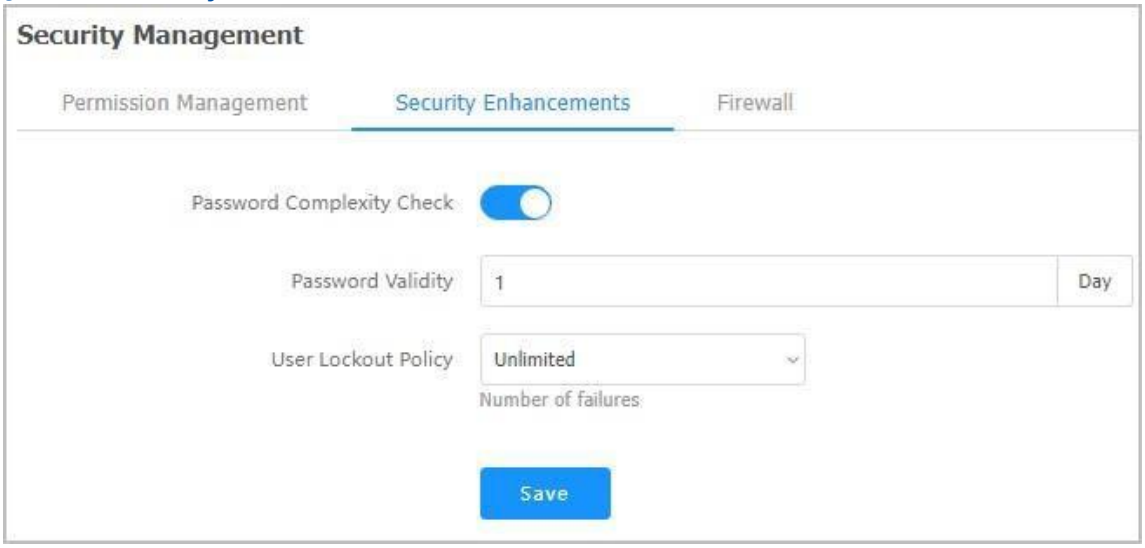
Kullanıcı oturum açma güvenliğini artırmak için, aşağıdaki güvenlik geliştirme parametrelerini yapılandırabilirsiniz:

- **Password Complexity Check**
- **Password Validity**
- **User Lockout Policy**

Adımlar

1. **User & Security** seçimini yapın. **User& Security** sayfası görüntülenir.
2. Sol taraftaki navigasyon ağacından, **Security Management** seçimini yapın. **Security Management** sayfası görüntülenir.
3. **Security Enhancements** üzerine tıklayın. **Security Enhancements** sayfası görüntülenir, bakınız Şekil 9-8.

Şekil 9-8 Security Enhancements Sekmesi



4. Parametreleri ayarlayın. Parametrelerin açıklamaları için, Tablo 9-6'ya başvurun.

Tablo 9-6 Security Enhancement Parametre Açıklamaları

Parametre	Ayarlar
Password Complexity Check	Parola karmaşıklık kontrolünün etkinleştirilip etkinleştirilmeyeceğine karar vermek için aşağıdakileri gerçekleştirin. • Parola karmaşıklık kontrolünü etkinleştirmek için **Password Complexity Check** anahtarını açın. • Parola karmaşıklık kontrolünü devre dışı bırakmak için **Password Complexity Check** anahtarını kapatın.
Password Validity	Parola geçerlilik süresini girin. Aralık: 0– 365, birim: gün. Eğer parola geçerlilik süresi 0 ise, geçerlilik süresinde bir sınırlama yoktur.
User Lockout Policy	En fazla oturum açma hatası sayısını seçin ve kilitlenme süresini girin. Bu maksimum sayı aşıldığında kullanıcının oturumu kilitlenir.

5. **Save** üzerine tıklayın.

Sözlük

A/D

- Analogdan Dijitale (Analog to Digital)

AC

- Alternatif Akım (Alternating Current)

AD

- Aktif Dizin (Active Directory)

AES

- Gelişmiş Şifreleme Standardı (Advanced Encryption Standard)

API

- Uygulama Programlama Arayüzü (Application Programming Interface)

ASCII

- Bilgi Değişimi için Amerikan Standart Kodu (American Standard Code for Information Interchange)

BBU

- Pil Yedekleme Birimi (Battery Backup Unit)

BIOS

- Temel Girdi / Çıktı Sistemi (Basic Input/Output System)

BMC

- Temel Kart Yönetim Denetleyicisi (Baseboard Management Controller)

CD

- Kompakt Disk (Compact Disk)

CLI

- Komut Satırı Ara Yüzü (Command Line Interface)

CPU

- Merkezi İşlemci Birimi (Central Processing Unit)

CRPS

- Ortak Yedekli Güç Kaynakları (Common Redundant Power Supplies)

DCMI

- Veri Merkezi Yönetilebilirlik Arayüzü (Data Center Manageability Interface)

DHCP

- Dinamik Sunucu Yapılandırma İletişim Kuralı (Dynamic Host Configuration Protocol)

DNS

- Alan Adı Sunucusu (Domain Name Server)

DVD

- Sayısal Çok Yönlü Disk (Digital Versatile Disc)

EPLD

- Silinebilir Programlanabilir Mantık Cihazı (Erasable Programmable Logic Device)

FC

- Fiber Kanal (Fiber Channel)

FQDN

- Tam Nitelikli Alan Adı (Fully Qualified Domain Name)

FRU

- Alanda Değiştirilebilir Birim (Field Replaceable Unit)

FTP

- Dosya Transfer Protokolü (File Transfer Protocol)

GPIO

- Genel Amaçlı Girdi Çıktı (General Purpose Input Output)

GPU

- Grafik İşleme Birimi (Graphics Processing Unit)

GUI

- Grafik Kullanıcı Arayüzü (Graphical User Interface)

HD

- Sabit disk (Hard disk)

HTML

- Yardımlı İşaretleme Dili (HyperText Markup Language)

HTTP

- Yardımcı Metin Aktarma Protokolü (Hypertext Transfer Protocol)

HTTPS

- Güvenli Yardımcı Metin Aktarma Protokolü (Hypertext Transfer Protocol Secure)

HVDC

- Yüksek Gerilimli Doğru Akım (High-Voltage Direct Current)

I/O

- Girdi/Çıktı (Input/Output)

ID

- Kimlik (Identification)

IE

- Internet Explorer

IP

- İnternet Protokolü (Internet Protocol)

IPMI

- Akıllı Platform Yönetim Arayüzü (Intelligent Platform Management Interface)

IPv4

- İnternet Protokolü versiyon 4 (Internet Protocol Version 4)

IPv6

- İnternet Protokolü versiyon 6 (Internet Protocol Version 6)

JRE

- Java Çalışma Zamanı Ortamı (Java Runtime Environment)

KVM

- Klavye, Video ve Fare (Keyboard, Video and Mouse)

LAN

- Yerel Alan Şebekesi (Local Area Network)

LDAP

- Hafif Dizin Erişim Protokolü (Lightweight Directory Access Protocol)

LPC

- Düşük Sıralı Yol Bağlantısı (Lower order Path Connection)

LVDC

- Düşük Gerilimli Doğru Akım (Low-Voltage Direct Current)

MAC

- Medya Erişim Kontrolü (Media Access Control)

NCSI

- Şebeke Denetleyicisi Yan Bant Arayüzü (Network Controller Sideband Interface)

NIC

- Ağ Arayüz Kartı (Network Interface Card)

NMS

- Ağ Yönetim Sistemi (Network Management System)

NTP

- Network Time Protocol (Ağ Zaman Protokolü)

NVMe

- Hızlı Geçici Olmayan Bellek (Non-Volatile Memory Express)

OS

- İşletim Sistemi (Operating System)

PC

- Kişisel Bilgisayar (Personal Computer)

PCIe

- Hızlı Çevre Bileşeni Ara Bağlantısı (Peripheral Component Interconnect Express)

PECI

- Platform Ortam Denetim Arayüzü (Platform Environment Control Interface)

POST

- Açılışta Otomatik Sınama (Power-On Self-Test)

PWM

- Darbe Genişliği Modülasyonu (Pulse-Width Modulation)

PXE

- Önyükleme Öncesi Yürütme Ortamı (Preboot eXecution Environment)

RAID

- Bağımsız Disklerin Yedek Dizisi (Redundant Array of Independent Disks)

RMCP

- Uzaktan Yönetim Kontrolü Protokolü (Remote Management Control Protocol)

RPM

- Dakikadaki Devir Sayısı (Rotations Per Minute)

SAS

- Seri Bağlı SCSI (Serial Attached SCSI)

SEL

- Sistem Olay Günlüğü (System Event Log)

SFTP

- Güvenli Dosya Transfer Protokolü (Secure File Transfer Protocol)

SGPIO

- Seri GPIO (Serial GPIO)

SHA

- Güvenli Hash Algoritması (Secure Hash Algorithm)

SMBUS

- Sistem Yönetimi Veri Yolu (System Management BUS)

SMTP

- Basit Posta Aktarma Protokolü (Simple Mail Transfer Protocol)

SNMP

- Basit Şebeke Yönetim Protokolü (Simple Network Management Protocol)

SSH

- Güvenli Kabuk (Secure Shell)

SSL

- Güvenli Soket Katmanı (Secure Sockets Layer)

TCP

- İletim Kontrol Protokolü (Transmission Control Protocol)

TLS

- Taşıma Katman Güvenliği (Transport Layer Security)

UEFI

- Birleşik Genişletilebilir Donanım Yazılımı Arayüzü (Unified Extensible Firmware Interface)

UID

- Birim Tanımlama Işığı (Unit Identification Light)

USB

- Evrensel Seri Veri Yolu (Universal Serial Bus)

VLAN

- Sanal Yerel Alan Şebekesi (Virtual Local Area Network)

VNC

- Sanal Ağ Konsolu (Virtual Network Console)

XML

- Genişleyebilir İşaretleme Dili (Extensible Markup Language)

iSAC

- Bütünleşik Sunucu Yöneticisi Denetleyicisi (Integrated Server Administrator Controller)