TEKNİK NOT

Illumina Proactive ile uzak sistem tanılamayı ayarlama

illumina®

İçindekiler

Illumina Proactive ile işlem verimliliğini en üst düzeye çıkarma

Illumina, pek çok laboratuvar için temel sekanslama sistemlerini oluşturan geniş bir yeni nesil sekanslama (NGS) cihazları yelpazesi sağlamaktadır. İster büyük bir sekanslama merkezi ister tek cihazlı küçük bir araştırma laboratuvarı çalıştırın, güvenilir cihaz işlevi ve yönetimi, optimum kullanım ve maksimum iş hacmi için kritik önem taşımaktadır.

Illumina, laboratuvarların bu hedefi gerçekleştirmesine yardımcı olmak amacıyla proaktif bakımı etkinleştirmek üzere her bir çalıştırmaya ait cihaz performans verilerinin Illumina'ya gönderildiği bir uzak sistem tanılama hizmeti olan Illumina Proactive'i sağlamaktadır. Tüm Illumina sekanslama cihazları performans verilerini yakalamak üzere tasarlanmıştır ve performansı izlemek için kullanılan metrik türleri yazılım versiyonuna bağlı olarak değişiklik gösterir. Kullanıcılar Illumina Proactive'i etkinleştirerek daha doğru arıza tanılama ve arıza risklerini saptama sayesinde sorun gidermeyi kolaylaştırır. Ek olarak Illumina Proactive; cihazın çalışma süresini artırabilir, işlem verimliliğini iyileştirebilir ve kaynak kaybı riskini azaltabilir (Şekil 1). Bu teknik notta cihaz performansını izlemenin faydaları açıklanmakta, Illumina Proactive'i etkinleştirme talimatları sağlanmakta ve veri güvenliği konusunda sık sorulan sorular yanıtlanmaktadır.

Illumina Proactive Avantajları

Cihazın çalışma süresini en yüksek düzeye çıkarır

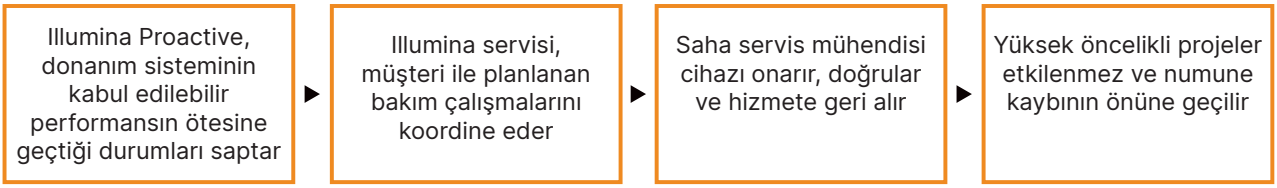
Yüksek arıza riski altındaki cihaz bileşenlerinin saptanması, planlanmamış kesinti süresini azaltabilir ve kullanıcıların gerekli bileşen değişimlerini kendileri için uygun bir zamanda planlamasına olanak sağlar. Bu özellik birkaç Illumina cihaz bileşeni için etkinleştirilmiştir ve diğer bileşenleri de kapsayacak şekilde genişletilmeye devam edilecektir.

Sorun giderme daha verimli şekilde çalışır

Bir sorunu gidermek için gereken bilgilerin yerini tespit etmek, bilgileri indirmek ve göndermek gereksiz gecikmelere yol açabilir. Diğer yandan Illumina Proactive aracılığıyla cihaz performansı parametrelerine doğrudan erişim sağlanması, Illumina Servis ve Destek ekibinin cihaz sorunlarını hızlı bir şekilde tanılamasına ve sorunları gidermesine olanak sağlar. Ek olarak geçmiş performansı izleme özelliği verimli bir şekilde sorun gidermeyi destekler ve kimi zaman önleyici cihaz onarımı sağlar.

Cihaz performans verileri nelerdir ve neden önemlidir?

Cihaz performans verileri; yazılım günlükleri, cihaz yapılandırmaları ve diğer dosya türleri dahil olmak üzere sekanslama cihazının işlem performansını karakterize edilebilecek her türlü metrik anlamına gelmektedir. Sekanslama verileri bu kategoride yer almamaktadır ve aynı veri akışı üzerinden sekanslama verilerine erişilemez ya da bu veriler raporlanamaz. Cihaz performans verileri çeşitli şekillerde arıza risk tahminini, arıza saptamayı ve performans sorunlarına ilişkin sorun gidermeyi destekleyebilir (Tablo 1).



Şekil 1: Illumina Proactive çalışması örneği—Bu örnekte, sistem performans verilerinin rutin izlemesi sonucunda optik donanım için arıza riski saptanır, yüksek öncelikli bir projeye yaklaşırken planlı bakım yapılması sağlanır. Potansiyel olarak yüksek maliyetli zaman, emek ve numune kayıplarının önüne geçilir.

Tablo 1: Çeşitli çalıştırma performans verileri türleri

Cihaz performans verileri	Çalıştırma performans verileri	Cihaz yapılandırma verileri	Çalıştırma yapılandırma verileri
Toplanan veriler	Q skorları, cihaz işlem günlükleri	Cihaz seri numarası, yazılım versiyonu	Çalıştırma parametreleri, reaktif ve akış hücresi lot numaraları
Illumina servis ekibi için değeri	Arıza tahmini, arıza saptama	Çalıştırma sorunlarını giderme	Çalıştırma sorunlarını giderme
Kullanıcı açısından değeri	Optik, mekanik, termal ve fluidik sistem performansına ilişkin hata ve uyarı bildirimlerinin analiz edilebilmesini sağlar	Yazılım versiyonu, cihaz türü veya diğer donanım değişkenlerinin performans sorunlarına yol açıp açmadığının değerlendirilmesini sağlar	Performans sorunlarına yol açan lot numarası, deney türü ve diğer deney değişkenlerinin rolleri hakkında bilgi sağlar

Illumina Proactive'i Etkinleştirme

Her bir sistem için cihaz performansını izleme özelliği kullanıcı tarafından denetim yazılımında yapılandırılır. Kullanıcı kılavuzlarında cihaz performans verilerinin iletilmesini etkinleştirmeye veya devre dışı bırakmaya ilişkin ayrıntılar sağlanmaktadır. Evrensel ve cihaza özgü ağ yapılandırmalarına ilişkin daha fazla bilgi için bu belgede yer alan Evrensel Ayarlar ve Cihaza Özgü Ayarlar bölümlerine bakın.

Illumina Proactive'in etkinleştirilmesine ilişkin gereklilikler:

- Giriş portu gerekmez
- Çıkış Portu 443
- Her bir bölge için BaseSpace™ Etki Alanları
- İlgili cihazlar için tesis hazırlama yönergelerinde belirtildiği şekilde bant genişliğine sahip ağ bağlantısı
- Yazılım, performans izlemeyi etkinleştirmek üzere yapılandırılmalıdır

Uç nokta gereklilikleri ve ağ oluşturma tavsiyelerine ilişkin ayrıntılar için bkz. support-docs.illumina.com/SHARE/NetworkSecurity/Content/SHARE/NetworkSecurity/SecurityIntro

Illumina Proactive'in etkinleştirilmesine ilişkin talimatlar:

1. Bilgi güvenliğine ilişkin tüm hususların, ilgili BT temsilcileri tarafından ele alındığından ve tüm kurumsal gerekliliklerin karşılandığından emin olun.

2. Geçerli sistemin cihaz performansını izleme ayarlarını onaylayın. Bazı cihazlarda bu özellik varsayılan olarak etkinleştirilmiş olabilir. Cihaz performansını izleme ayarlarına bakın.

3. Çalıştırma başlatmadan önce "Send Instrument Performance Data to Illumina" (Cihaz Performans Verilerini Illumina'ya Gönder) onay kutusunu seçin. Tam olarak bu sözcüklerle ifade edilmese de tüm Illumina cihazlarında kullanıcı arayüzünde bu seçenek sağlanmaktadır.

Veri güvenliği hususları

Veri güvenliği, Illumina müşterileri için birincil önceliklerden biridir. Illumina olarak genom ve diğer sağlık verilerinin gizliliği konusunda topluluğumuzda artan özeni kabul etmekte ve ürünlerimizi, bu değişen standartları karşılayacak şekilde tasarlamaktayız. Yeni sistemler tasarlanıp yeni bilgi tehditleri tanımlandıkça, tutarlı çalışmaların bir sonucu olarak Illumina işletim sistemlerinin güvenlik profilleri zamanla daha da gelişmektedir. Illumina, siber güvenlik bakımından güçlü duruşunu korumak ve sağlık sektöründeki inovasyonları desteklemek amacıyla, ortaya çıkan yeni tehditlere göre sistem güvenlik profillerini sürekli olarak değerlendirmekte ve geliştirmektedir. Genom verileri dahil olmak üzere müşterilerin kişisel bilgilerinin gizliliğinin korunması Illumina uygulamalarının esasını oluşturmaktadır.

Giriş portu yoktur

Illumina sekanslama sistemleri internetten giriş portları gerektirmez. Illumina bu portların engellenmesini tavsiye eder. Bu işlem, internet üzerinden oturum açma ekranına erişme olasılığını azaltır. Bu güvenlik önlemi uzak konumlardan işletim sistemine erişimi azaltır.

Yazılım kısıtlama politikası

Pek çok Illumina sistemi, Illumina bilgisayarlarında çalıştırılan uygulamaları Illumina onaylı (izin listesinde yer alan) uygulamalarla sınırlandıran yazılım kısıtlama politikası (SRP) özelliğine sahiptir. Herhangi bir kötü amaçlı yazılım sisteme sızsa bile kullanıcı dosyaları nasıl görürse görsün (yani kötü amaçlı yazılım, görüntü dosyası ya da excel elektronik tablosu olarak görünebilir) SRP koruması, dosyaların yürütülmesine izin vermeyeceği için bu kısıtlama tüm kötü amaçlı yazılımların yürütülmesi olasılığını azaltır.

Geçiş sırasında güvenlik

Cihazlar, BaseSpace™ Sequence Hub ile web tabanlı uygulama program arayüzü (API) üzerinden iletişim kurar. Sekanslama cihazı ile BaseSpace Sequence Hub arasındaki tüm trafikte, hassas iletişimleri internet üzerinden geçerken şifreleyen bir internet standardı olan Taşıma Katmanı Güvenliği (TLS 1.2) kullanılır. Tüm servis yöntemlerinde API anahtar imzaları gereklidir ve diğer tümü için servis reddedilir.

Durağan modda şifreleme

Kalıcı depolama sistemlerinde depolanan veriler "durağan" olarak nitelendirilir. BaseSpace Sequence Hub durağan verileri korumak için Gelişmiş Şifreleme Sistemini (Advanced Encryption System; AES)-256 kullanır. AES-256, ABD National Institutes of Standards and Technology (NIST) tarafından oluşturulan elektronik veri şifreleme spesifikasyonudur.[2]

Veri merkezi güvenliği

Illumina Proactive Amazon Web Services (AWS) tarafından sunulan mevcut Illumina bulut altyapısı ile entegredir. Verilere güvenli erişim, bulut uygulamaları paketi için yıllık ISO 27001:2013 denetim sertifikası[3] ve Sağlık Sigortası Taşınabilirlik ve Sorumluluk Yasası (HIPAA) tasdiki (AT101) verilen Illumina BaseSpace Sequence Hub kullanılarak yönetilir.[4,5] Illumina Proactive çözümünden faydalanmak için BaseSpace Sequence Hub hesabınızın olması gerekmez.

Illumina software as a service (hizmet olarak yazılım–SaaS) ürünleri, Genel Veri Koruma Yönetmeliği (GDPR) dahil olmak üzere veri koruma ve veri işlemeye ilişkin en iyi uygulamalara ve yasalara uyumluluk sağlamak üzere tasarlanmıştır ve bu doğrultuda uygulanmaktadır. Müşteriler, kendi kişisel verilerinin kullanımına ilişkin GDPR sorumluluklarını belirlemelidir. Illumina'nın bulut veri güvenliği ve gizlilik uygulamalarına ilişkin daha ayrıntılı bilgiye Illumina bulut veri güvenliği sayfasından ulaşabilirsiniz. Bulut hizmet sağlayıcı veri güvenliği uygulamaları için AWS Veri Koruma Sayfası'na bakın.

Veri güvenliği hakkında sık sorulan sorular

S: Illumina Proactive'i etkinleştirirsem sekans verilerim Illumina'ya gönderilir mi?

Y: Hayır. Cihaz yalnızca, daha önce açıklandığı şekilde yazılım günlüklerini ve cihaz yapılandırmalarını içeren cihaz performans verilerini Illumina'ya gönderir. Sekanslama çalıştırma verileri gönderilmez ve verilere bu hizmet üzerinden erişilmez. Cihaz performansını izleme ile sekans verileri analizi arasındaki bağlantıyı ayrıştırmak için çeşitli özelliklerden yararlanılabilir (Tablo 2).

Tablo 2: BaseSpace Sequence Hub bağlantı seçenekleri

Nitelik	Illumina Proactive modu	Çalıştırmayı izleme modu	BaseSpace Sequence Hub Analysis modu
Bağlantı türü	Tek seferlik cihaz yapılandırması	Çalıştırma öncesi kullanıcı bağlantısı	Çalıştırma başına kullanıcı bağlantısı
İnternet bağlantısı gerektirir	✓	✓	✓
Cihaz yapılandırması ve işlem günlükleri dahildir[a]	✓	✓	✓
BaseSpace Sequence Hub oturumunun açılmasını gerektirir		✓	✓
Sekans verileri (BCL) dosyalarını içerir			✓

a. Özel cihaz yapılandırması ve işlem günlüklerine ilişkin ayrıntılar için lütfen Ek'te yer alan cihaza özgü ayarlar bölümüne başvurun.

S: Cihaz performans verilerimi Illumina'ya göndermem her türlü arıza risklerinin proaktif olarak saptanmasını sağlayacak mı?

Y: Hayır. Cihaz performansını izleme özelliği şimdiye dek çok sayıda vakada proaktif bakım yapılabilmesini sağlamıştır. Daha fazla veri elde edildikçe bu hizmetin özellikleri Illumina sekanslama ürün yelpazesi genelinde daha kapsamlı hale getirilecek ve daha üst düzeye taşınacaktır.

S: Bu hizmeti etkinleştirmek için BaseSpace Sequence Hub oturumumu açmam gerekecek mi?

Y: Hayır. Cihaz performans verileri modu için yalnızca Illumina ağ bağlantısı gereklidir. Cihaz performans verileri ve sekanslama verileri birbirinden bağımsız olarak gönderildiğinden BaseSpace Sequence Hub oturumunuzu açmanız gerekmez.

S: Bilgi Güvenliği ekibim, bu hizmet etkinleştirilmeden önce daha fazla teknik bilgi istemektedir. İlave kaynak var mı?

Y: Evet. Illumina cihazları ve Proactive yazılımı hakkında veri güvenliği hususlarının ele alındığı ve genel veri güvenliği en iyi uygulamalarının sunulduğu ilave kaynaklar bulunmaktadır. Illumina Teknik Destek birimine techsupport@illumina.com adresinden ulaşabilirsiniz.

Illumina veri güvenliği uygulamaları hakkında bilgi için Illumina Güvenlik web sayfasını ziyaret edin veya Kurumsal Gizlilik Politikamızı gözden geçirin. NGS sistemlerimize ve bulut tabanlı SaaS ürünlerimize özgü veri güvenliği belgeleri için Ek'e bakın.

S: Illumina Proactive, GDPR'ye uygun mu?

Y: Evet. Illumina SaaS ürünleri, GDPR dahil olmak üzere global yasalara uygun şekilde tasarlanmıştır ve bu doğrultuda çalıştırılmaktadır.

S: Veri güvenliği konusunda Illumina tarafından tavsiye edilen başka en iyi uygulamalar var mı?

Y: Sadece araştırma amaçlı cihazların ve tanı amaçlı tıbbi cihazların güvenli şekilde kullanıma alınması, güvenlik katmanlarına bağlıdır. Illumina, cihazların güvenilir cihazlarla birlikte en küçük ağ alt ağında ya da güvenlik bağlamında kullanıma alınmasını kesinlikle tavsiye etmektedir. Gelen ve giden bağlantı erişimlerini kısıtlamak için güvenlik duvarları ve diğer ağ politikaları kullanılmalıdır. Hassas verilerin korunmasını sağlamak için deneylerden veya numune kimliklerinden numuneye özgü bilgilerin de çıkarılması gerekmektedir.

Ek

Kalan kısımlarda, BT departmanınızın Illumina Proactive'i uygulamak için bilmesi gereken gereklilikler belirtilmektedir.

Ağ yapılandırması

Illumina Proactive'i uygulamak veya BaseSpace Sequence Hub ile entegrasyon sağlamak adına tüm Illumina sistemlerinde birden fazla ortak entegrasyon ayarı bulunmaktadır ancak her bir platformun, kullanım amacına bağlı olarak platforma özgü gereklilikleri de olabilir. Illumina, hem evrensel bağlantı gereklilikleri (tüm ILMN platformlarında ortak bağlantılar) için güncellenmiş bir konum hem de her bir platforma özgü ayarları sunmaktadır.

Ağ oluşturmaya ilişkin diğer tavsiyeler dahil olmak üzere daha fazla bilgi için şu adresi ziyaret edin: support-docs.illumina.com/SHARE/NetworkSecurity/Content/SHARE/NetworkSecurity/SecurityIntro

Denetim bilgisayarı güvenlik duvarı

Windows güvenlik duvarı, potansiyel tehditleri gidermek için gelen trafiği filtreleyerek denetim bilgisayarını korur. Güvenlik duvarı varsayılan olarak gelen tüm bağlantıları engellemek üzere etkinleştirilmiştir. Güvenlik duvarını etkin tutun ve tüm giden bağlantılara izin verin.

İhtiyaç duyulan uç noktalar hakkında daha fazla bilgi için şu adresi ziyaret edin: support-docs.illumina.com/SHARE/NetworkSecurity/Content/SHARE/NetworkSecurity/SecurityIntro

Local Run Manager haricinde giriş portları gerekli değildir veya tavsiye edilmez. Uzak Masaüstü Protokolü (RDP) bazı sistemlerde varsayılan olarak etkinleştirilebilir ve Local Run Manager'ın yerel izin listesi için gereklilik olarak listelenmediği durumlarda RDP dahil olmak üzere tüm giriş portlarının kapatılması tavsiye edilir. Local Run Manager internet erişimi gerektirmez; yalnızca yerel depolama ve yönetim kaynaklarına erişim gereklidir. Illumina Güvenlik En İyi Uygulamaları Kılavuzu, güvenlik duvarları ve RDP hakkında daha fazla bilgi sağlamaktadır.

Anti-virüs yapılandırması

Cihaz denetim bilgisayarını virüslere karşı korumak için kullanıcı tarafından seçilen bir anti-virüs yazılımının kullanılması kesinlikle tavsiye edilir. Veri kaybı veya kesintisini önlemek için anti-virüs yazılımını aşağıdaki gibi yapılandırın:

- Manuel taramaları ayarlayın; otomatik taramalara izin vermeyin
- Manuel taramaları yalnızca cihaz kullanımda değilken yapın
- Güncellemeleri kullanıcı yetkilendirmesi olmadan indirilecek ancak yüklenmeyecek şekilde ayarlayın
- Cihazı çalışırken güncellemeyin; yalnızca cihazın çalışmadığı ve cihaz denetim bilgisayarının güvenle yeniden başlatılabileceği durumlarda güncelleyin
- Güncellemeden sonra bilgisayarı otomatik olarak yeniden başlatmayın
- Uygulama dizinini ve veri sürücülerini gerçek zamanlı dosya sistem korumasının dışında tutun; bu ayarı C:\Illumina ve Z:\ilmn dizinlerine uygulayın
- Windows Defender'ı devre dışı bırakın; bu Windows ürünü, Illumina yazılımı tarafından kullanılan işletim sistemi kaynaklarını etkileyebilir

İşletim sistemi yapılandırmaları

Illumina cihazları gönderimden önce spesifikasyonlar dahilinde işlev gösterip göstermediği açısından test edilmiş ve doğrulanmıştır. Kurulum sonrasında bu ayarlar üzerinde herhangi bir değişiklik yapılması performans ya da güvenlik risklerine yol açabilir. Aşağıdaki yapılandırma tavsiyeleri, işletim sistemine ilişkin performans ve güvenlik risklerini en aza indirmektedir:

- En az 10 karakterlik bir parola yapılandırın ve ek kılavuzluk için yerel numaralandırma politikalarından yararlanın; parolayı kaydedin
- Illumina müşterilerin oturum açma kimlik bilgilerini saklamamaktadır ve bilinmeyen parolalar sıfırlanamaz
- Parolanın bilinmemesi halinde bir Illumina temsilcisinin fabrika varsayılanlarını geri yüklemesi gerekir ve bu, sistemdeki tüm verilerin silinmesine ve gereken destek süresinin uzamasına neden olur
- Güncellemeleri önlemek üzere Windows'ta Otomatik Güncellemeleri Yapılandırın
- Grup İlkesi Nesneleri (GPO'lar) ile bir etki alanına bağlantı sağlandığında bazı ayarlar işletim sistemini veya cihaz yazılımını etkileyebilir; cihaz yazılımı hatalı şekilde işlev gösterirse olası GPO girişimi konusunda tesisinizin BT yöneticisine danışın
- Windows güvenlik duvarı veya ağ güvenlik duvarını (donanım veya yazılım) kullanın ve Uzak Masaüstü Protokolünü (RDP) devre dışı bırakın; güvenlik duvarları ve RDP hakkında daha fazla bilgi için Illumina Güvenlik En İyi Uygulamaları Kılavuzuna bakın[5]
- Kullanıcılar için yönetici ayrıcalıklarını koruyun; Illumina cihaz yazılımı, cihaz gönderildiğinde kullanıcı izinlerine olanak sağlayacak şekilde yapılandırılmıştır
- Sistem sabit dahili IP adresleri içermektedir ve bu, çakışmalar meydana geldiğinde sistem arızasına yol açabilir
- Denetim bilgisayarı, Illumina sekanslama sistemlerini çalıştırmak üzere tasarlanmıştır; internette dolaşmak, e-postaları kontrol etmek, belgeleri incelemek ve diğer sekanslama dışı aktiviteler kalite ve güvenlik sorunlarına yol açar

Windows güncellemeleri

Illumina yalnızca kritik güvenlik güncellemelerinin uygulanmasını tavsiye eder. Cihaz denetim bilgisayarının yapılandırmasını ve işlevini kontrol etmek ve daha sağlam bir çalışma ortamı sağlamak amacıyla varsayılan Windows işletim sisteminin Windows Update özelliği kapalıdır. Sistemde özellik güncellemelerinin ya da genel güncellemelerin yapılması sistemin çalışma ortamını riske atabilir ve bu desteklenmemektedir. Illumina Güvenlik En İyi Uygulamaları Kılavuzu Windows Update alternatifleri hakkında daha fazla bilgi sağlamaktadır.

Üçüncü taraf yazılımı

Illumina kurulumda sağlananların dışındaki yazılımları desteklememektedir. Sistemle birlikte sağlanmayan Chrome, Java, Box veya diğer herhangi bir üçüncü taraf yazılımını kurmayın. Üçüncü taraf yazılımları test edilmemiştir ve performans ve güvenlik açısından engellere yol açabilir. Örneğin, RoboCopy veya diğer senkronizasyon ve akış programları denetim yazılımı ürün paketi tarafından gerçekleştirilen akış ile girişim oluşturduğundan sekanslama verilerinin bozulmasına ya da eksik olmasına yol açabilir.

Kullanıcı davranışı

Cihaz denetim bilgisayarı, Illumina sekanslama sistemlerini çalıştırmak üzere tasarlanmıştır. Genel amaçlı bilgisayar olarak kullanılmamalıdır. Kalite ve güvenlik nedenleriyle, denetim bilgisayarının internette dolaşmak, e-postaları kontrol etmek, belgeleri incelemek veya diğer gereksiz aktiviteler için kullanılması kesinlikle tavsiye edilmez ve bu tür bir kullanım, düşük performansa ya da veri kaybına neden olabilir.

Grup ilkesi uygulaması

Grup İlkesi Nesneleri (GPO) içeren bir etki alanına bağlandığınızda bazı ayarlar işletim sistemini veya cihaz yazılımını etkileyebilir (Tablo 3). Cihaz yazılımı hatalı şekilde işlev gösterirse olası GPO girişimi konusunda tesisinizin BT yöneticisine danışın.

Parola yönetimi

En az 12 karakterlik bir parola yapılandırın ve ek kılavuzluk için yerel numaralandırma politikalarından yararlanın. Parolayı kaydedin. Müşteri güvenliği için, Illumina müşterilerin oturum açma kimlik bilgilerini saklamamaktadır ve bilinmeyen parolalar sıfırlanamaz. Parolanın bilinmemesi halinde bir Illumina temsilcisinin fabrika varsayılanlarını geri yüklemesi gerekir ve bu, sistemdeki tüm verilerin silinmesine ve gereken destek süresinin uzamasına neden olur.

Yönetici hakları ve ayrıcalıkları

Kullanıcılar için yönetici ayrıcalıklarını koruyun. Illumina cihaz yazılımı, cihaz gönderildiğinde kullanıcı izinlerine olanak sağlayacak şekilde yapılandırılmıştır.

Tablo 3: Dahili sistem işlemleri için evrensel onay gereklilikleri

Bağlantı	Değer	Amaç
Etki Alanı	localhost:*	Yerel ana makineler arası iletişime yönelik tüm portlar; işlemler arası iletişim için gereklidir
Port	8081	Gerçek zamanlı analiz
Port	8080	Denetim yazılımı
Port	8090	Uzak kopya hizmeti

Cihaza özgü ayarlar

Önceki bölümlerde belirtilen ayarların yanı sıra her bir platform için göz önünde bulundurulması gereken ve izin listesine alınması gereken dahili ayarları temsil eden ayarlar bulunmaktadır (Tablo 4, Tablo 5).

Tablo 4: Illumina sekanslama sistemlerine ilişkin bilgi güvenliği spesifikasyonları

Sistem	SRP	EMET	Varsayılan IPD ayarı	Tercih Etme veya Vazgeçme	Yazılım yükseltmesinde IPD ayarı
NovaSeq 6000	Evet	Evet	Açık	Vazgeçme	Önceki ayarı koruma
HiSeq serisi	Hayır	Hayır	Açık	Vazgeçme	Açık olarak sıfırlama
NextSeq 550	Hayır	Hayır	Açık	Vazgeçme	Önceki ayarı koruma
NextSeq 550Dx - Research Mode	Evet	Evet	Kapalı	Tercih etme	Önceki ayarı koruma
NextSeq 1000 ve NextSeq 2000	Hayır	Hayır	Açık	Vazgeçme	Önceki ayarı koruma
MiSeq	Hayır	Hayır	Açık	Vazgeçme	Önceki ayarı koruma (kullanıcı bazında)
MiSeqDx	Hayır	Hayır	Kapalı	Tercih etme	Önceki ayarı koruma
MiSeqDx - Research Mode	Hayır	Hayır	Açık	Vazgeçme	Önceki ayarı koruma
MiniSeq	Hayır	Hayır	Açık	Vazgeçme	Önceki ayarı koruma
iSeq 100	Evet	Hayır	Açık	Vazgeçme	Önceki ayarı koruma
iScan	Hayır	Hayır	Açık	Vazgeçme	Önceki ayarı koruma (kullanıcı bazında)

Local Run Manager modülünün bulunduğu sistemlerde yalnızca yerel ağ için Port 80 veya 443'ün giriş portu olması gereklidir

Tablo 5: Sisteme göre dahili iletişim gereklilikleri

Sistem	Portlar ve IP adresleri	Amaç	Bant genişliği gerekliliği
NovaSeq 6000	5555	Donanım denetleyici arayüzü	200 Mb/sistem
	22, 80, 111, 443, 623, 2049, 5900, 8889, 9980, 169.254.x.x, fddc:65e5:66fa::1/48, fddc:65e5:66fa::2/48	Dahili veri transferi	200 Mb/sistem
HiSeq serisi	HiSeq System dahili IP iletişim süreçleri içermemektedir		100 Mb/sistem
NextSeq 550	192.168.113.*:*	Tüm Portlara İzin Verin; dahili ağ kartında donanım yazılımı içeren iletişim bağlantısıdır	50 Mb/sistem
NextSeq 550Dx	192.168.113.*:*	Tüm Portlara İzin Verin; dahili ağ kartında donanım yazılımı içeren iletişim bağlantısıdır	50 Mb/sistem
	Port 80 veya 443	Local Run Manager; gereken yerel giriş (internet erişimi olmadan)	50 Mb/sistem
NextSeq 1000 ve NextSeq 2000	21, 22, 4647, 5458, 5555, 5647, 7359, 7360, 169.254.*.*.*	Tüm Portlara İzin Verin; dahili ağ kartında donanım yazılımı içeren iletişim bağlantısıdır	200 Mb/sistem
MiSeq	Port 80 veya 443	Local Run Manager; gereken yerel giriş (internet erişimi olmadan)	10 Mb/sistem
MiSeqDx	Port 80 veya 443	Local Run Manager; gereken yerel giriş (internet erişimi olmadan)	10 Mb/sistem
MiniSeq	192.168.113.*:*	Tüm Portlara İzin Verin; dahili ağ kartında donanım yazılımı içeren iletişim bağlantısıdır	10 Mb/sistem
	Port 80 veya 443	Local Run Manager; gereken yerel giriş (internet erişimi olmadan)	10 Mb/sistem
iSeq 100	Port 80 veya 443	Local Run Manager; gereken yerel giriş (internet erişimi olmadan)	10 Mb/sistem
iScan	6030, 888	AutoLoader	10 Mb/sistem

Listelenen IP kritiktir; donanım denetleyicisi için arayüzdür.

İletişim gerekliliklerine ilişkin daha fazla bilgi için söz konusu sistemin Tesis Hazırlama Yönergelerine bakın (Tablo 6). Her sistemin kullanıcı kılavuzları, cihaz yazılımı üzerinden IPD'nin etkinleştirilmesine ilişkin bilgileri içermektedir (Tablo 6).

Tablo 6: Illumina sistemlerine ilişkin kullanıcı kılavuzları ve tesis hazırlama yönergeleri

Sistem	Sistem/referans kılavuz	Tesis hazırlama yönergeleri
NovaSeq 6000	1000000019358	1000000019360
HiSeq 1000	15023355	15006407
HiSeq 1500	15035788	15006407
HiSeq 2000	15011190	15006407
HiSeq 2500	15035786	15006407
HiSeq 3000	15066493	15066492
HiSeq 4000	15066496	15066492
HiSeq X	15050091	15050093
NextSeq 500	15046563	15045113
NextSeq 550	15069765	15045113
NextSeq 550Dx	1000000009513	1000000009869
NextSeq 1000 ve NextSeq 2000	1000000109376	1000000109378
MiSeq	15027617	15027615
MiSeqDx	15070067	15038351
MiniSeq	1000000002695	1000000002696
iSeq 100	1000000036024	1000000035337
iScan	11313539	1000000000661

Güncellemeler nedeniyle köprü bağlantısı devre dışı kalırsa kılavuzun daha yeni bir versiyonunu bulmak üzere Illumina web sitesinde arama yapmak için sağlanan belge numarası kullanılabilir.

Cihaz performans verilerinin türleri

Tablo 7: Cihaz performans verilerinin türleri (cihaz yapılandırma dosyaları)

Dosya adı	Dosya açıklaması	iScan	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
Effective.cfg	Yazılım sistemini yapılandırmaya ilişkin toplam parametreler	X	X	X	X		X	X	X	X	X	X	X
FirmwareVersions.txt	Cihaz donanımındaki donanım yazılımı versiyonu						X			X	X		X
*Calibration.cfg	Yazılım sistemi kalibrasyon parametreleri	X					X	X		X	X	X	X
*Override.cfg	Yazılım sistemini yapılandırmaya ilişkin geçersiz kılma parametreleri	X	X	X	X		X			X	X	X	X
RTAStart.bat	Birincil analiz başlangıç dosyası					X	X			X	X		
Options.cfg	Yazılım sistemini yapılandırmaya ilişkin geçersiz kılma parametreleri												X
*HardwareHistory.csv	Cihaz donanımı yapılandırma geçmişi						X			X	X		
*CurrentHardware.csv	Cihaz donanımı güncel yapılandırması						X			X	X		
Sequencing Configuration.xml	Cihaz sistemi yapılandırma parametreleri					X							
Channel*cc.txt	Kamera kalibrasyon dosyası	X											

a. HiSeq 1000, 1500, 2000 ve 2500 System.

Tablo 8: Cihaz performans verilerinin türleri (cihaz işlem günlükleri)

Dosya adı	Dosya türü	Dosya açıklaması	iScan	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
*.jpg	Çalıştırmaya özgü işlem görüntüleri	Seçenek (varsayılan olarak etkin değildir) etkinleştirilmişse (genellikle FAS/FSE tarafından etkinleştirilir) her bir kutu ve renk kanalı için küçük resim görüntüsü						X	X	X	X	X		
Samplesheet.csv	Çalıştırmaya özgü numune yapılandırma dosyası	Sekanslama numune sayfası												X[b]
Recipe file (XML)	Çalıştırmaya özgü yapılandırma dosyası	Çalıştırmada kullanılan sekanslama reçetesi					X					X	X	X
Logs.zip		Okunabilir dosyalardan oluşan sıkıştırılmış klasör; müşteriler tüm dosyalara cihaz üzerinde erişebilir					X	X	X	X	X	X	X	X
CompressedLogs.zip		Günlük dosyalarının sıkıştırılmış koleksiyonu; müşteriler tüm dosyalara cihaz üzerinde erişebilir	X											

a. HiSeq 1000, 1500, 2000 ve 2500 System.
b. Numune sayfası artık NovaSeq 6000 v1.6 yazılımına yüklenmemektedir.

Tablo 9: Cihaz performans verilerinin türleri (cihaz analitikleri yapılandırma dosyaları)

Dosya adı	Dosya açıklaması	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
RTAConfiguration.xml	RTA yapılandırması	X	X	X	X	X	X	X		X		
RTA3.cfg	RTA yapılandırması										X	X
RTAerror.txt	Birincil analiz hata günlük dosyası					X	X					

a. HiSeq 1000, 1500, 2000 ve 2500 System.

Tablo 10: Cihaz performans verilerinin türleri (çeşitli dosya türleri)

Dosya adı	Dosya açıklaması	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
*.IMF logs	Yazılıma ilişkin işlem günlüğü dosyaları		X	X		X				X	X	X
*Results.zip	Servis yazılımı test sonuçları; bu, yalnızca servis yazılımında bir Servis ve Destek personeli tarafından tetiklendiğinde gönderilir					X			X	X	X	

a. HiSeq 1000, 1500, 2000 ve 2500 System.

Tablo 11: Cihaz performans verilerinin türleri (çalıştırmaya özgü işlem günlükleri)

Dosya adı	Dosya açıklaması	iScan	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
*Firmware_Logs	Donanım yazılımı işlem günlüğü dosyaları (.csv)						X			X	X		
PreRunDiagnostic Files	Sekanslama öncesi çalıştırma denetim sonuçları ve günlük dosyaları (.csv ve .xml)					X	X			X	X	X	X
Cycle Logs	Döngü başına oluşturulan işlem verilerine ilişkin sorun giderme günlükleri (.txt ve .xml formu)						X	X	X	X	X	X	X
Error.log	İşlem verilerine ilişkin sorun giderme günlükleri		X	X	X							X	X
CycleTimes.txt	Sekanslama çalıştırması sırasında döngü süresi		X	X	X								
UCS Logs	Kopya hizmeti günlük dosyası (.json ve .csv)												X
CycleTime.tsv	Döngü ve tarama süresi günlük dosyası	X											
*.scrst	BeadChip tarama ayarları yapılandırma dosyası	X											

a. HiSeq 1000, 1500, 2000 ve 2500 System.

Tablo 12: Cihaz performans verilerinin türleri (çalıştırmaya özgü analitik dosyaları)

Dosya adı	Dosya açıklaması	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
RTAComplete.txt	Tüm birincil işlemenin tamamlandığını gösteren dosya	X	X	X	X	X	X	X	X	X	X	X
RTARead*Complete.txt	Birincil işlemenin önemli adımı tamamladığını gösteren dosya				X							
RunParameters.xml	Çalıştırmanın başında XML formunda çıktı olarak sunulan çalıştırma ayarları yapılandırma parametreleri	X	X	X	X	X	X	X	X	X	X	X
RunInfo.xml	Sequencing Analysis Viewer için kullanılan çalıştırmanın başında XML formunda çıktı olarak sunulan çalıştırma ayarları yapılandırma parametreleri	X	X	X	X	X	X	X	X	X	X	X
RunCompletionStatus.xml	Tüm sekanslamanın tamamlandığını gösteren gösterge dosyası	X	X	X		X	X	X	X	X	X	X
SequenceComplete.txt	Tüm sekanslamanın tamamlandığını gösteren gösterge dosyası											X
*MetricsOut.bin	Sequencing Analysis Viewer için ikili raporlama dosyaları; müşteri ek yazılım olmadan okuyamaz	X	X	X	X	X	X	X	X	X	X	X
AlignmentMetricsOut.bin					X						X	X
BasecallingMetricsOut.bin					X						X	X
CorrectedIntMetricsOut.bin	Ortalama yoğunluk, düzeltilmiş kanal yoğunluğu, düzeltilmiş aranan yoğunluk, aranan sayılar	X	X	X	X	X	X	X	X	X	X	X
EmpiricalPhasingMetrics Out.bin	Fazlama, döngü başına prefaz	X	X	X	X	X	X	X	X	X	X	X
ErrorMetricsOut.bin	Hata oranı, okuma hataları	X	X	X	X	X	X	X	X		X	X
EventMetricsOut.bin	RTA başlangıcı, döngü başlangıcı, şablon oluşturma başlangıcı/tamamlama, şablon sonrası maksimum küme başlatma, gigabayt cinsinden kullanılabilir sistem belleği, kayıt ve ekstraksiyon, komşu düzeltme, renk matriksi düzeltme, şablon oluşturma, baz arama ve kalite skoru, sekans hizalama, bcl yazma, okuma başlangıcı/ tamamlama, filtre hizalama başlangıcı/tamamlama, döngü tamamlama, RTA tamamlama zamanlama verileri	X	X	X	X	X	X	X	X	X	X	X
ExtendedTileMetricsOut.bin					X						X	X
ExtrationMetricsOut.bin	Focus skorları, yoğunluklar, zaman	X	X	X	X		X	X	X	X	X	X
FWHMGridMetricsOut.bin					X						X	X
ImageMetricsOut.bin					X						X	X
IndexMetricsOut.bin	Ad, numune adı, proje adı				X		X				X	X
OpticalModeMetricsOut.bin											X	X
PFGrtidMetricsOut.bin	Küme sayısı, PF küme sayısı, mm^2 cinsinden Locs alanı	X	X	X	X		X	X	X	X	X	X
QMetrics2030Out.bin					X		X					X
QMetricsByLaneOut.bin					X		X					X
QMetricsOut.bin	Q skoru histogramı	X	X	X	X		X	X	X		X	X
RegistrationMetricsOut.bin	Alt kutu ofsetleri, afin dönüşüm	X	X	X			X	X	X		X	X
TileMetricsOut.bin	Küme yoğunluğu, küme yoğunluğu PF, küme sayısı, küme sayısı PF, hizalama yüzdesi, fazlama yüzdesi, prefaz yüzdesi, son ekstrakte edilen döngü, son aranan döngü, son Q skoru verilen döngü, son hata döngüsü	X	X	X	X		X	X	X	X	X	X
*.tsv veya *.txt	RTA dosyası kopya günlükleri, genel günlükler ve uyarı günlükleri için oluşturulan TSV veya TXT günlük dosyaları; müşteriler okunabilir biçimde erişebilir				X		X	X	X	X		
QGridMetricsOut.bin					X							
ReconstructionMetricsOut. bin											X	

Referanslar

1. Microsoft Security Response Center. msrc.microsoft.com. Erişim Tarihi: 12 Nisan 2023.
2. National Institute of Standards and Technology. Advanced Encryption Standard (AES). csrc.nist.gov/publications/detail/fips/197/final. Yayınlanma Tarihi: 1 Kasım 2001. Erişim Tarihi: 12 Nisan 2023.
3. Amazon. AWS: ISO/IEC 27001:2013. aws.amazon.com/compliance/iso-27001-faqs/. Erişim Tarihi: 12 Nisan 2023.
4. Illumina. (2018) BaseSpace Sequence Hub Güvenlik ve Gizlilik. illumina.com/content/dam/illumina/gcs/assembled-assets/marketing-literature/basespace-security-and-privacy-security-brief-m-gl-01959/basespace-security-and-privacy-security-brief-m-gl-01959.pdf. Erişim Tarihi: 8 Kasım 2023.

illumina®

1 800 809 4566 ücretsiz (ABD) | +1 858 202 4566 tel
techsupport@illumina.com | www.illumina.com

M-GL-01092 TUR v2.0