TEKNISK ANTECKNING

Ställa in fjärrsystem-diagnostik med Illumina Proactive

illumina®

Innehållsförteckning

Maximera effektiviteten med Illumina Proactive

Illumina erbjuder ett brett sortiment av nästa generations sekvenseringsinstrument (NGS) som har blivit de huvudsakliga sekvenseringssystemen i många laboratorier. Oavsett om användaren arbetar i ett stort sekvenseringscenter eller ett mindre forskningslabb med ett enda instrument, är tillförlitlig instrumentdrift och -hantering avgörande för optimal användning och maximal kapacitet.

För att hjälpa laboratorier med att uppnå det här målet tillhandahåller Illumina därför Illumina Proactive, en fjärrsystemdiagnostiktjänst där instruments prestandadata från varje körning skickas till Illumina för att möjliggöra proaktivt underhåll. Alla sekvenseringsinstrument från Illumina är konstruerade för att registrera prestandadata, men vilken typ av mätning som används för att övervaka prestandan varierar beroende på programvaruversion. Genom att aktivera Illumina Proactive förbättras felsökningen med mer exakt feldiagnostik och riskdetektering. Dessutom kan Illumina Proactive förlänga instrumentets drifttid, förbättra effektiviteten och minska risken att resurser går förlorade (Figur 1). I det här tekniska dokumentet listas fördelarna med övervakning av instruments prestanda, anvisningar för hur du aktiverar Illumina Proactive samt svar på vanliga frågor om datasäkerhet.

Fördelar med Illumina Proactive

Maximera instrumentets drifttid

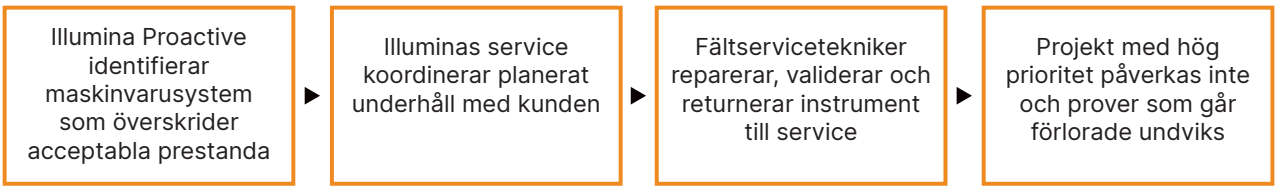
Om du upptäcker instrumentkomponenter med förhöjd risk för fel så kan det minska oplanerat driftstopp och göra det möjligt för användare att schemalägga nödvändiga komponentbyten vid behov. Den här funktionen har aktiverats för flera olika instrumentkomponenter från Illumina och kommer att fortsätta utvecklas för andra.

Effektivare felsökning

Det kan orsaka onödiga förseningar att hitta, ladda ner och skicka nödvändig information för att felsöka ett problem. Å andra sidan ger direktåtkomst till instrumentets prestandaparametrar genom Illumina Proactive Illuminas service- och supportteam möjlighet att snabbt diagnostisera och felsöka instrumentproblem. Dessutom främjar prestandaövervakning effektiv felsökning och ibland även förebyggande instrumentreparationer.

Vad är instrumentets prestandadata och varför är de viktiga?

Instrumentets prestandadata innebär alla typer av mätningar som kan karakterisera sekvenseringsinstrumentets driftprestanda, inklusive programvaruloggar, instrumentkonfigurationer och andra filtyper. Sekvenseringsdata ingår inte i den här kategorin och är inte tillgängliga och rapporteras inte via samma dataström. Instrumentets prestandadata kan underlätta felriskberäkning, feldetektering och felsökning av prestandaproblem på olika sätt (Tabell 1).



Figur 1: Exempel på Illumina Proactive i bruk. I detta exempel resulterar rutinmässig övervakning av systemprestandadata i att felrisk för optisk hårdvara upptäcks, vilket leder till planerat underhåll kring ett högt prioriterat projekt. En eventuell kostsam förlust av tid, arbete och prover undviks.

Tabell 1: Olika typer av prestandadata för körning

Instrumentets prestandadata	Prestandadata för körning	Instrumentets konfigurationsdata	Konfigurationsdata för körning
Data som samlas in	Q-poäng, instrumentets operativa loggar	Instrumentets serienummer, programvaruversion	Körparametrar, reagens och flödescellslotantal
Fördelar för Illuminas serviceteam	Felberäkning, feldetektering	Felsökning av körning	Felsökning av körning
Fördel för användaren	Möjliggör analys av felmeddelanden och varningar om prestanda i optiska, mekaniska, termiska och flödestekniska system	Möjliggör bedömning av huruvida programvaruversion, instrumenttyp eller andra maskinvaruvariabler kan vara bidragande till prestandaproblem	Informerar om hur lotnummer, experimenttyp och andra experimentella variabler bidrar till prestandaproblem

Aktivera Illumina Proactive

Övervakningen av instrumentets prestanda konfigureras av användaren för varje system i kontrollprogrammet. I användarhandböckerna finns information om hur du aktiverar eller inaktiverar överföringen av instrumentets prestandadata. Mer utförlig information om universella och instrumentspecifika nätverkskonfigurationer finns i avsnitten Universella inställningar och Instrumentspecifika inställningar i det här dokumentet.

Aktiveringskrav för Illumina Proactive:

- Inga ingående portar krävs
- Utgående port 443
- BaseSpace™-domäner för varje region
- Nätverksanslutning med bandbredd som anges i förberedelseguider för plats för specifika instrument
- Programvara måste konfigureras för att aktivera prestandaövervakning

För information om slutpunktkrav och nätverksrekommendationer, se support-docs.illumina.com/SHARE/NetworkSecurity/Content/SHARE/NetworkSecurity/SecurityIntro

Anvisningar för att aktivera Illumina Proactive:

1. Säkerställ att eventuella frågor om informationssäkerhet hanteras av lämpliga IT-representanter och att alla institutionella skyldigheter uppfylls.

2. Bekräfta de aktuella instrumentinställningarna för prestandaövervakning. Vissa instrument kan ha funktionen aktiverad som standard. Se instrumentinställningar för prestandaövervakning.

3. Markera kryssrutan ”Send Instrument Performance Data to Illumina” (Skicka instrumentets prestandadata till Illumina) innan en körning inleds. Det här alternativet finns i användargränssnittet för alla Illumina-instrument, men den exakta formuleringen kan variera något.

Att tänka på gällande datasäkerhet

Datasäkerhet är högsta prioritet för Illuminas kunder. Illumina är medveten om det ökade fokuset i vårt samhälle på integriteten för genomisk och annan hälsodata och vi utformar våra produkter för att uppfylla dessa standarder i ständig utveckling. Tack vare ett kontinuerligt arbete förbättras säkerhetsprofilerna för Illuminas operativsystem hela tiden, allteftersom nya system utformas och nya hot identifieras. Illumina utvärderar och förbättrar kontinuerligt sina systemsäkerhetsprofiler när nya hot identifieras för att upprätthålla en stark cybersäkerhetsställning och stödja kontinuerlig innovation inom hälsovården. Grundläggande för Illumina-metoder är att skydda integriteten för kundens personuppgifter, inklusive genomiska data.

Inga ingående portar

Sekvenseringssystem från Illumina kräver inte ingående internetportar. Illumina rekommenderar att sådana portar blockeras, vilket minskar möjligheten att komma åt inloggningsskärmen via internet. Den här säkerhetsåtgärden minskar alltså fjärråtkomsten till operativsystemet.

Princip som begränsar programvara

Många Illumina-system har en funktion som kallas Software Restriction Policy (Princip för begränsning av programvara) (SRP) och som begränsar program som körs på Illumina-datorer till de som Illumina har godkänt (listade som tillåtna). Den här begränsningen minskar sannolikheten för att skadlig kod körs, även om den infiltrerar systemet, eftersom SRP-skydd inte tillåter körning – oavsett hur filerna visas för användaren (dvs. skadlig kod kan visas som en bildfil eller ett Excel-kalkylark).

Säkerhet vid överföring

Instrument kommunicerar med BaseSpace Sequence Hub via ett webbaserat programmeringsgränssnitt (API). All trafik mellan sekvenseringsinstrumentet och BaseSpace Sequence Hub använder Transport Layer Security (TLS 1.2), ett internetprotokoll som krypterar känslig information när den överförs via internet. Alla servicemetoder kräver API-nyckelsignaturer, annars nekas service.

Kryptering av vilande data

Data som lagras i fasta lagringssystem kallas ”vilande”. BaseSpace Sequence Hub använder Advanced Encryption System (AES)-256 för att skydda vilande data. AES-256 är en standard för kryptering av elektroniska data som skapats av amerikanska National Institutes of Standards and Technology (NIST).[2]

Säkerhet tack vare datacenter

Illumina Proactive kan integreras med befintlig Illumina-molninfrastruktur som tillhandahålls av Amazon Web Services (AWS). Säker åtkomst till data hanteras med Illumina BaseSpace Sequence Hub, vars svit med molnapplikationer har uppnått årlig ISO 27001:2013 revisionscertifiering[3] och attestering för sjukförsäkringsportabilitet och ansvarsskyldighet (HIPAA) (AT101).[4,5] Det behövs inget BaseSpace Sequence Hub-konto för Illumina Proactive.

Illumina-programvara som en tjänst (SaaS) är konstruerad och körs i enlighet med bästa praxis och lagstiftning för dataskydd och -hantering, inklusive den allmänna dataskyddsförordningen (GDPR). Kunder bör fastställa GDPR-ansvar för användning av sina egna personuppgifter. Mer information om Illuminas molndatasäkerhet och sekretesspraxis finns på Illuminas molndatasäkerhetssida. För datasäkerhetspraxis för molntjänster, se AWS dataskyddssida.

Vanliga frågor om datasäkerhet

F: Kommer mina sekvensdata att skickas till Illumina om jag aktiverar Illumina Proactive?

S: Nej. Det är endast instrumentets prestandadata, som de programvaruloggar och instrumentkonfigurationer som beskrivits tidigare, som skickas till Illumina via instrumentet. Data om sekvenseringskörning skickas inte och går inte att komma åt via den här tjänsten. Anslutningen mellan övervakningen av instrumentets prestanda och sekvensdataanalys särskiljs av olika funktioner (Tabell 2).

Tabell 2: Anslutningsalternativ för BaseSpace Sequence Hub

Funktion	Illumina Proactive-läge	Läge för körningsövervakning	Analysläge för BaseSpace Sequence Hub
Anslutningstyp	Engångskonfiguration av instrument	Användaranslutning innan körning	Användaranslutning per körning
Kräver en internetanslutning	✓	✓	✓
Inkluderar instrumentkonfiguration och arbetsloggar [a]	✓	✓	✓
Kräver BaseSpace Sequence Hub-inloggning		✓	✓
Inkluderar filer med sekvensdata (BCL)			✓

a. Mer information om specifik instrumentkonfiguration och arbetsloggar finns i avsnittet Instrumentspecifika inställningar i bilagan.

F: Aktiveras proaktiv detektering av alla typer av felrisker om jag skickar mitt instruments prestandadata till Illumina?

S: Nej. Däremot har övervakning av instruments prestanda möjliggjort proaktivt underhåll i många olika fall. Allteftersom fler data blir tillgängliga, kommer tjänstens kapacitet att fortsätta utökas och förbättras i Illuminas sortiment av sekvenseringsprodukter.

F: Måste jag logga in på min BaseSpace Sequence Hub för att aktivera den här tjänsten?

S: Nej. Du behöver endast en nätverksanslutning till Illumina för att använda läget med instrumentets prestandadata. Eftersom instrumentets prestandadata och sekvenseringsdata skickas oberoende av varandra krävs ingen BaseSpace Sequence Hub-inloggning.

F: Mitt informationssäkerhetsteam behöver ytterligare teknisk information för att aktivera den här tjänsten. Finns det ytterligare resurser tillgängliga?

S: Ja. Ytterligare resurser finns tillgängliga som adresserar datasäkerhetshänsyn för Illuminas instrument och proaktiv programvara och ger allmänna bästa metoder för datasäkerhet. Illuminas teknisk support kan nås på techsupport@illumina.com.

För mer information om Illuminas datasäkerhetspraxis kan du besöka Illumina Securitys webbsida eller läsa vår företagsintegritetspolicy. Se bilagan för datasäkerhetsdokumentation som är specifik för våra NGS-system och molnbaserade SaaS-produkter.

F: Uppfyller Illumina Proactive kraven i GDPR-lagarna?

S: Ja. Illuminas SaaS-produkter är konstruerade och körs i enlighet med global lagstiftning, inklusive GDPR.

F: Rekommenderar Illumina några andra rutiner gällande datasäkerhet?

S: Säker implementering av instrument endast för forskningsbruk och diagnostiska medicinska apparater beror på säkerhetsskikt. Illumina rekommenderar starkt att instrument och enheter används i den minsta nätverksundergruppen eller säkerhetskontexten, med betrodda enheter. Brandväggar och andra nätverkspolicyer bör användas för att begränsa inkommande och utgående åtkomst. Provspecifik information bör också utelämnas från namnen på experiment eller prov-ID för att hålla känsliga data skyddade.

Bilaga

Resterande avsnitt innehåller information om krav som din IT-avdelning måste känna till för att implementera Illumina Proactive.

Nätverkskonfiguration

Flera integrationsinställningar är gemensamma för alla Illumina-system för att implementera Illumina Proactive eller integrera med BaseSpace Sequence Hub, men varje plattform kan också ha krav som är specifika för den plattformen, beroende på avsett användningsfall. Illumina tillhandahåller en uppdaterad plats för både universella anslutningskrav (anslutningar som är gemensamma för alla ILMN-plattformar) och inställningar specifika för varje plattform.

För mer information, inklusive andra rekommendationer för nätverk, besök support-docs.illumina.com/SHARE/NetworkSecurity/Content/SHARE/NetworkSecurity/SecurityIntro

Kontrolldatorns brandvägg

Windows brandvägg skyddar kontrolldatorn genom att filtrera inkommande trafik för att ta bort potentiella hot. Brandväggen är aktiverad som standard för att blockera alla inkommande anslutningar. Håll brandväggen aktiverad och tillåt utgående anslutningar.

För mer information om de nödvändiga slutpunkterna, besök support-docs.illumina.com/SHARE/NetworkSecurity/Content/SHARE/NetworkSecurity/WindowsFirewall

Ingående portar varken krävs eller rekommenderas, förutom för Local Run Manager. Remote Desktop Protocol (RDP) kan vara aktiverat som standard i vissa system och rekommendationen är att stänga alla ingående portar, även RDP, såvida inte Local Run Manager anges som ett krav för lokal listning som tillåtna. Local Run Manager kräver ingen internetanslutning, bara tillgång till lokala lagrings- och hanteringsresurser. Mer information om brandväggar och RDP finns i Illuminas guide för bästa säkerhetspraxis.

Antiviruskonfiguration

Vi rekommenderar att du använder valfritt antivirusprogram för att skydda instrumentets kontrolldator mot virus. Undvik dataförlust eller avbrott genom att konfigurera antivirusprogrammet på följande sätt:

- Ställ in för manuella skanningar, tillåt inte automatiska skanningar
- Utför endast manuella genomsökningar när instrumentet inte används
- Ställ in att uppdateringar ska laddas ned utan användarens godkännande men inte installeras
- Uppdatera inte under instrumentdrift, uppdatera endast när instrumentet inte körs och när det är säkert att starta om instrumentets kontrolldator
- Starta inte om datorn automatiskt vid uppdatering
- Exkludera programkatalogen och dataenheterna från eventuella filsystemsskydd som utförs i realtid, tillämpa den här inställningen på katalogerna C:\Illumina och Z:\ilmn
- Inaktivera Windows Defender. Den här Windows-produkten kan påverka de operativsystemsresurser som Illumina-programvaran använder

Operativsystemskonfigurationer

Instrument från Illumina testas och bekräftas fungera inom specifikationerna före transport. Om inställningarna ändras efter installation kan det leda till funktions- eller säkerhetsrisker. Följande rekommenderade konfigurationer minskar funktions- och säkerhetsriskerna för operativsystemet:

- Ställ in ett lösenord som består av minst 10 tecken och använd lokala ID-principer för att få ytterligare hjälp. Spara lösenordet
- Illumina lagrar inte användarnas inloggningsuppgifter och det går inte att återställa bortglömda lösenord
- Om ett lösenord glömts bort måste en representant från Illumina återställa fabriksinställningarna, vilket raderar alla data från systemet och förlänger supporttiden
- Konfigurera automatiska uppdateringar i Windows så att uppdateringar förhindras
- Om du ansluter till en domän med grupprincipobjekt (GPO) kan vissa inställningar påverka operativsystemet eller instrumentets programvara. Om instrumentprogramvaran fungerar felaktigt, konsultera IT-administratören för din inrättning om möjlig GPO-interferens
- Använd Windows brandvägg eller en nätverksbrandvägg (hårdvara eller programvara) och inaktivera Remote Desktop Protocol (RDP). För mer information om brandväggar och RDP, se Illuminas guide för bästa säkerhetspraxis[5]
- Upprätthålla administrativa rättigheter för användare. Illumina-instruments programvara är konfigurerad till att ge användarbehörigheter när instrumentet skickas
- Systemet har fasta interna IP-adresser, vilket kan orsaka systemfel när konflikter uppstår
- Kontrolldatorn är konstruerad för att köra sekvenseringssystem från Illumina. Webbsurfande, läsning av e-post, granskning av dokument och andra aktiviteter som inte gäller sekvensering skapar kvalitets- och säkerhetsproblem

Windows-uppdateringar

Illumina rekommenderar att endast kritiska säkerhetsuppdateringar genomförs. För att kunna kontrollera konfigurationen och driften av kontrolldatorn och få en stabilare driftmiljö är Windows Update inaktiverat i standardoperativsystemet från Windows. Funktionsuppdateringar och allmänna uppdateringar kan utsätta systemets driftmiljö för risk och stöds därför inte. Mer information om alternativ för Windows-uppdateringar finns i Illuminas guide för bästa säkerhetspraxis.

Programvara från tredje part

Illumina stöder inte någon programvara utöver den som tillhandahålls vid installationen. Installera inte Chrome, Java, Box eller någon annan programvara från tredje part som inte medföljde systemet. Programvara från tredje part har inte testats och kan störa funktion och säkerhet. Exempelvis kan RoboCopy eller andra synkroniserings- och strömningsprogram leda till att sekvenseringsdata skadas eller saknas eftersom programmet stör den strömning som utförs av kontrollprogramsviten.

Användarbeteende

Instrumentets kontrolldator är konstruerad för att köra sekvenseringssystem från Illumina. Den ska inte användas för andra syften. Av kvalitets- och säkerhetsskäl ska du inte använda kontrolldatorn till att surfa på nätet, läsa e-post, granska dokument eller till någon annan onödig aktivitet, då det kan resultera i försämrade prestanda och förlorade data.

Tillämpning av grupprincip

Om du ansluter till en domän med grupprincipobjekt (GPO) kan vissa inställningar påverka operativsystemet eller instrumentets programvara (Tabell 3). Om instrumentets programvara inte fungerar korrekt kan du rådfråga den IT-ansvariga om eventuell interferens av GPO:er.

Lösenordshantering

Ställ in ett lösenord som består av minst 12 tecken och använd lokala ID-principer för att få ytterligare hjälp. Skriv ned och spara lösenordet. Av säkerhetsskäl lagrar Illumina inte användarnas inloggningsuppgifter och det går inte att återställa bortglömda lösenord. Om ett lösenord glömts bort måste en representant från Illumina återställa fabriksinställningarna, vilket raderar alla data från systemet och förlänger supporttiden.

Administrativa rättigheter och behörigheter

Bibehåll administrativa rättigheter för användare. Illumina-instruments programvara är konfigurerad till att ge användarbehörigheter när instrumentet skickas.

Tabell 3: Universella godkännandekrav för intern systemdrift

Anslutning	Värde	Användningsområde
Domän	localhost:*	Alla portar för localhost-till-localhost-kommunikation som behövs för interprocesskommunikation
Port	8081	Realtidsanalys
Port	8080	Kontrollprogram
Port	8090	Fjärrkopieringstjänst

Instrumentspecifika inställningar

Utöver de inställningar som nämnts ovan finns det inställningar som måste övervägas för varje plattform, t.ex. interna inställningar som måste listas som tillåtna (Tabell 4, Tabell 5).

Tabell 4: Informationssäkerhetsspecifikationer för Illuminas sekvenseringssystem

System	SRP	EMET	Standard-IPD-inställning	Aktivera eller inaktivera	IPD-inställning vid programvaruuppgradering
NovaSeq 6000	Ja	Ja	På	Inaktivera	Behåller tidigare inställning
HiSeq-serien	Nej	Nej	På	Inaktivera	Återställer till På
NextSeq 550	Nej	Nej	På	Inaktivera	Behåller tidigare inställning
NextSeq 550Dx – forskningsläge	Ja	Ja	Av	Aktivera	Behåller tidigare inställning
NextSeq 1000 och NextSeq 2000	Nej	Nej	På	Inaktivera	Behåller tidigare inställning
MiSeq	Nej	Nej	På	Inaktivera	Behåller tidigare inställning (på användarnivå)
MiSeqDx	Nej	Nej	Av	Aktivera	Behåller tidigare inställning
MiSeqDx – forskningsläge	Nej	Nej	På	Inaktivera	Behåller tidigare inställning
MiniSeq	Nej	Nej	På	Inaktivera	Behåller tidigare inställning
iSeq 100	Ja	Nej	På	Inaktivera	Behåller tidigare inställning
iScan	Nej	Nej	På	Inaktivera	Behåller tidigare inställning (på användarnivå)

System med Local Run Manager-modulen kräver att port 80 eller 443 endast är ingång för det lokala nätverket.

Tabell 5: Interna kommunikationskrav efter system

System	Portar och IP-adresser	Användningsområde	Bandbreddskrav
NovaSeq 6000	5555	Gränssnitt för maskinvarustyrenhet	200 Mb/system
	22, 80, 111, 443, 623, 2049, 5900, 8889, 9980, 169.254.x.x, fddc:65e5:66fa::1/48, fddc:65e5:66fa::2/48	Intern dataöverföring	200 Mb/system
HiSeq-serien	HiSeq-systemet har inga interna IP-kommunikationsprocesser		100 Mb/system
NextSeq 550	192.168.113.*:*	Tillåt alla portar. Det här är kommunikationslänken till den inbyggda programvaran på det interna nätverkskortet	50 Mb/system
NextSeq 550Dx	192.168.113.*:*	Tillåt alla portar. Det här är kommunikationslänken till den inbyggda programvaran på det interna nätverkskortet	50 Mb/system
	Port 80 eller 443	Local Run Manager. Obligatorisk lokal ingång (ingen internetanslutning)	50 Mb/system
NextSeq 1000 och NextSeq 2000	21, 22, 4647, 5458, 5555, 5647, 7359, 7360, 169.254.*.*.*	Tillåt alla portar. Det här är kommunikationslänken till den inbyggda programvaran på det interna nätverkskortet	200 Mb/system
MiSeq	Port 80 eller 443	Local Run Manager. Obligatorisk lokal ingång (ingen internetanslutning)	10 Mb/system
MiSeqDx	Port 80 eller 443	Local Run Manager. Obligatorisk lokal ingång (ingen internetanslutning)	10 Mb/system
MiniSeq	192.168.113.*:*	Tillåt alla portar. Det här är kommunikationslänken till den inbyggda programvaran på det interna nätverkskortet	10 Mb/system
	Port 80 eller 443	Local Run Manager. Obligatorisk lokal ingång (ingen internetanslutning)	10 Mb/system
iSeq 100	Port 80 eller 443	Local Run Manager. Obligatorisk lokal ingång (ingen internetanslutning)	10 Mb/system
iScan	6030, 888	AutoLoader	10 Mb/system

IP-listan är kritisk. Det är gränssnittet för hårdvarukontrollern.

Mer information om kommunikationskrav finns i förberedelseguiden för det specifika systemets plats (Tabell 6). Användarhandböckerna för varje specifikt system innehåller information och anvisningar för att aktivera IPD via instrumentprogramvara (Tabell 6).

Tabell 6: Användarhandböcker och förberedelseguider för plats för Illumina-system

System	System/referensguide	Förberedelseguide för plats
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 och NextSeq 2000	1000000109376	1000000109378
MiSeq	15027617	15027615
MiSeqDx	15070067	15038351
MiniSeq	1000000002695	1000000002696
iSeq 100	1000000036024	1000000035337
iScan	11313539	1000000000661

Om en hyperlänk bryts till följd av uppdateringar kan du använda det angivna dokumentnumret för att söka efter en nyare version av handboken eller guiden på Illuminas webbplats.

Instrumentets prestandadatatyper

Tabell 7: Instrumentets prestandadatatyper (konfigurationsfiler)

Filnamn	Filbeskrivning	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	Totala parametrar för konfiguration av programvarusystem	X	X	X	X		X	X	X	X	X	X	X
FirmwareVersions.txt	Version av instrumentets inbyggda programvara						X			X	X		X
*Calibration.cfg	Kalibreringsparametrar för programvarusystem	X					X	X		X	X	X	X
*Override.cfg	Åsidosättningsparametrar för konfiguration av programvarusystem	X	X	X	X		X			X	X	X	X
RTAStart.bat	Fil för primär analysstart					X	X			X	X		
Options.cfg	Åsidosättningsparametrar för konfiguration av programvarusystem												X
*HardwareHistory.csv	Konfigurationshistorik för instrumentets hårdvara						X			X	X		
*CurrentHardware.csv	Nuvarande konfiguration av instrumentets hårdvara						X			X	X		
Sequencing Configuration.xml	Parametrar för instrumentets systemkonfiguration					X							
Channel*cc.txt	Fil för kamerakalibrering	X											

a. HiSeq 1000-, 1500-, 2000- och 2500-system.

Tabell 8: Instrumentets prestandadatatyper (arbetsloggar för instrument)

Filnamn	Filtyp	Filbeskrivning	iScan	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
*.jpg	Körningsspecifika arbetsbilder	Miniatyrbild för varje titel och färgkanal om alternativet har aktiverats i programvaran (inaktiverat som standard). Aktiveras vanligtvis av FAS/FSE						X	X	X	X	X		
Samplesheet.csv	Körningsspecifik provkonfigurationsfil	Sekvenseringsprovark												X[b]
Receptfil (.xml)	Körningsspecifik konfigurationsfil	Sekvenseringsrecept som används vid körning					X					X	X	X
Logs.zip		Komprimerad mapp med läsbara filer som är lättillgängliga för kunden via instrumentet					X	X	X	X	X	X	X	X
CompressedLogs.zip		Komprimerad mapp med loggfiler som är lättillgängliga för kunden via instrumentet	X											

a. HiSeq 1000-, 1500-, 2000- och 2500-system.
b. Provark överförs inte längre i NovaSeq 6000 v1.6-programvaran.

Tabell 9: Instrumentets prestandadatatyper (instrumentets analyskonfigurationsfiler)

Filnamn	Filbeskrivning	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-konfiguration	X	X	X	X	X	X	X		X		
RTA3.cfg	RTA-konfiguration										X	X
RTAerror.txt	Felloggfil för primär analys					X	X					

a. HiSeq 1000-, 1500-, 2000- och 2500-system.

Tabell 10: Instrumentets prestandadatatyper (diverse filtyper)

Filnamn	Filbeskrivning	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
*.IMF logs	Arbetsloggfiler för programvara		X	X		X				X	X	X
*Results.zip	Testresultat för tjänsteprogram – skickas endast om funktionen aktiveras av service- och supportpersonal via ett tjänsteprogram					X			X	X	X	

a. HiSeq 1000-, 1500-, 2000- och 2500-system.

Tabell 11: Instrumentets prestandadatatyper (körningsspecifika arbetsloggar)

Filnamn	Filbeskrivning	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	Arbetsloggfiler för inbyggd programvara (.csv)						X			X	X		
PreRunDiagnostic Files	Kontrollresultat och loggfiler för försekvenseringskörning (.csv och .xml)					X	X			X	X	X	X
Cycle Logs	Felsökningsloggar för arbetsdata som genereras per cykel (.txt och .xml)						X	X	X	X	X	X	X
Error.log	Felsökningsloggar för arbetsdata		X	X	X							X	X
CycleTimes.txt	Cykeltid under en sekvenseringskörning		X	X	X								
UCS Logs	Loggfil för Universal Copy Service (.json och .csv)												X
CycleTime.tsv	Loggfil för cykel- och skanningstid	X											
*.scrst	Konfigurationsfil för BeadChip-skanningsinställningar	X											

a. HiSeq 1000-, 1500-, 2000- och 2500-system.

Tabell 12: Instrumentets prestandadatatyper (körningsspecifika analysfiler)

Filnamn	Filbeskrivning	HiSeq[a]	HiSeq 3000/4000	HiSeq X	iSeq 100	MiniSeq	MiSeq	MiSeqDx	NextSeq 500/550	NextSeq 550Dx	NextSeq 1000/2000	NovaSeq 6000
RTAComplete.txt	Indikatorfil som indikerar att all primär bearbetning har slutförts	X	X	X	X	X	X	X	X	X	X	X
RTARead*Complete.txt	Indikatorfil som indikerar att den primära bearbetningen har slutfört ett nyckelsteg				X							
RunParameters.xml	Ställ in konfigurationsparametrar i XML-format i början av körningen	X	X	X	X	X	X	X	X	X	X	X
RunInfo.xml	Ställ in konfigurationsparametrar i XML-format i början av körningen som används för Sequencing Analysis Viewer	X	X	X	X	X	X	X	X	X	X	X
RunCompletionStatus.xml	Indikatorfil som indikerar när sekvenseringen är slutförd	X	X	X		X	X	X	X	X	X	X
SequenceComplete.txt	Indikatorfil som indikerar när sekvenseringen är slutförd											X
*MetricsOut.bin	Binära rapporteringsfiler för Sequencing Analysis Viewer som inte kan läsas av kunden utan ytterligare programvara	X	X	X	X	X	X	X	X	X	X	X
AlignmentMetricsOut.bin					X						X	X
BasecallingMetricsOut.bin					X						X	X
CorrectedIntMetricsOut.bin	Genomsnittlig intensitet, korrigerad kanalintensitet, korrigerad bestämd intensitet, bestämt antal	X	X	X	X	X	X	X	X	X	X	X
EmpiricalPhasingMetricsOut.bin	Fasning, förfasning per cykel	X	X	X	X	X	X	X	X	X	X	X
ErrorMetricsOut.bin	Felfrekvens, läsfel	X	X	X	X	X	X	X	X		X	X
EventMetricsOut.bin	Tidsdata för RTA har startats, cykel har startats, skapande av mall har startats/slutförts, mall efter initiering av maximalt antal kluster, tillgängliga gigabyte i systemminnet, registrering och extrahering, korrigering av angränsande, korrigering av färgmatris, skapande av mall, basbestämning och kvalitetsbedömning, sekvenslinjering, skriva bcl-fil, läsning har startats/slutförts, filterlinjering har startats/slutförts, cykel har slutförts, RTA har slutförts	X	X	X	X	X	X	X	X	X	X	X
ExtendedTileMetricsOut.bin					X						X	X
ExtrationMetricsOut.bin	Fokusresultat, intensiteter, tid	X	X	X	X		X	X	X	X	X	X
FWHMGridMetricsOut.bin					X						X	X
ImageMetricsOut.bin					X						X	X
IndexMetricsOut.bin	Namn, provnamn, projektnamn				X		X				X	X
OpticalModeMetricsOut.bin											X	X
PFGrtidMetricsOut.bin	Klusterantal, antal kluster som passerar filtret, Locs-område i mm^2	X	X	X	X		X	X	X	X	X	X
QMetrics2030Out.bin					X		X					X
QMetricsByLaneOut.bin					X		X					X
QMetricsOut.bin	Histogram med Q-resultat	X	X	X	X		X	X	X		X	X
RegistrationMetricsOut.bin	Subtila förskjutningar, affin transformering	X	X	X			X	X	X		X	X
TileMetricsOut.bin	Klusterdensitet, densitet för kluster som passerar filtret, klusterantal, antal kluster som passerar filtret, procent inpassade, procent fasning, procent förfasning, senaste extraherade cykeln, senaste bestämda cykeln, senaste cykeln med kvalitetsresultat, senaste felcykeln	X	X	X	X		X	X	X	X	X	X
*.tsv eller *.txt	TSV- eller TXT-loggfiler som genereras för RTA-filkopieringsloggar, globala loggar och varningsloggar som är tillgängliga för kunden i läsbart format				X		X	X	X	X		
QGridMetricsOut.bin					X							
ReconstructionMetricsOut.bin											X	

Referenser

1. Microsoft Security Response Center. msrc.microsoft.com. Öppnat den 12 juli 2022.
2. National Institute of Standards and Technology. Advanced Encryption Standard (AES). csrc.nist.gov/publications/detail/fips/197/final. Publicerat den 1 november 2001. Öppnat den 12 juli 2022.
3. Amazon. AWS: ISO/IEC 27001:2013. aws.amazon.com/compliance/iso-27001-faqs/. Öppnat den 12 juli 2022.
4. Illumina. (2018) BaseSpace Sequence Hub Security and Privacy. illumina.com/content/dam/illumina-marketing/documents/products/whitepapers/basespace-sequence-hub-security-and-privacy-white-paper-970-2016-020.pdf. Öppnat den 12 juli 2022.

illumina®

1 800 809 45 66 kostnadsfritt (USA) | +1 858 202 45 66 tel
techsupport@illumina.com | www.illumina.com

M-GL-01092 SWE v1.0