Galddatora pārvaldības rokasgrāmata

Biznesa datori

Galddatora pārvaldības rokasgrāmata

Biznesa datori

Trešais izdevums (2008. gada jūlijs)

Dokumenta daļas numurs: 451272-E13

Par šo grāmatu

Šajā rokasgrāmatā ir sniegtas definīcijas un norādījumi par drošības un inteliģentās pārvaldības līdzekļiem, kas ir sākotnēji instalēti atsevišķiem modeļiem.

⚠ **BRĪDINĀJUMS!** Šādi izcelts teksts nozīmē, ka norādījumu neievērošanas gadījumā iespējams gūt fiziskas traumas vai var tikt apdraudēta dzīvība.

△ **UZMANĪBU!** Šādi izcelts teksts nozīmē, ka, neievērojot norādījumus, var sabojāt aparatūru vai zaudēt informāciju.

PIEZĪME Šādi tiek izcelts teksts ar svarīgu papildinformāciju.

Saturs

1 Pārskats par galddatora pārvaldību

HP pārvaldības risinājums Client Management Solutions nodrošina standarta risinājumus galddatoru, darbstaciju un piezīmjdatoru pārvaldībai un kontrolei tīkla vidē. 1995. gadā kompānija HP sāka datoru pārvaldību, ieviešot nozarē pirmos pilnībā pārvaldāmos galddatorus. HP pieder pārvaldības tehnoloģijas patents. Kopš tā laika HP ir nozares vadošais uzņēmums, izstrādājot standartus un infrastruktūru, kas nepieciešama efektīvai galddatoru, darbstaciju un piezīmjdatoru ieviešanai, konfigurēšanai un pārvaldībai. HP izstrādā savu pārvaldības programmatūru un cieši sadarbojas ar nozares vadošajiem programmatūras risinājumu sniedzējiem, lai nodrošinātu HP klientu pārvaldības risinājumu un šo produktu saderību. HP klientu pārvaldības risinājumi ir svarīgs darbības veids mūsu plašajos centienos piedāvāt jums risinājumus, kas palīdz samazināt datoru kopējās uzturēšanas izmaksas visā to kalpošanas laikā.

Galvenās galddatora pārvaldības funkcijas un līdzekļi:

- Sākotnējā konfigurācija un ieviešana
- Attālā sistēmas instalēšana
- Programmatūras jaunināšana un pārvaldība
- Pārrakstāmā ROM
- Aparatūras opciju konfigurācija
- Datu izsekošana un drošība
- Kļūdu paziņojumi un atkopšana

PIEZĪME Atsevišķu šajā rokasgrāmatā aprakstīto līdzekļu atbalsts var atšķirties atkarībā no modeļa vai programmatūras versijas.

2 Sākotnējā konfigurācija un izvietojums

Dators ir aprīkots ar sākotnēji instalētu sistēmas programmatūras attēlu. Pēc īsa programmatūras “atpakošanas” procesa dators ir gatavs lietošanai.

Iespējams, jūs vēlēsities aizstāt sākotnēji instalēto programmatūras attēlu ar pielāgotu sistēmas un lietojumprogrammu kopu. Pielāgotu programmatūras attēlu var ieviest vairākos veidos. Tie ir:

- Pēc sākotnēji instalētās programmatūras attēla atpakošanas, instalējot papildu lietojumprogrammas.
- Programmatūras izvietošanas rīku izmantošana, piemēram, HP Client Automation Standard Edition, HP Client Automation Enterprise Edition (pamatā Radia tehnoloģija) vai Altiris Deployment Solution, lai jau instalēto programmatūru aizstātu ar pielāgotas programmatūras attēlu.
- Klonējot diskus, lai viena cietā diska saturu pārkopētu citā cietajā diskā.

Labākā ieviešanas metode ir atkarīga no informāciju tehnoloģiju vides un procesiem.

Sistēma HP Backup and Recovery, uz ROM pamatotais iestatījums un ACPI aparatūra nodrošina tālāku palīdzību ar sistēmas programmatūras atkopšanu, konfigurācijas pārvaldību un problēmu novēršanu, un strāvas pārvaldību.

PIEZĪME Informāciju par atkopšanas disku komplektu izveidi skatiet sadaļā HP Backup and Recovery Manager 11. lpp. .

HP programmatūras aģents

Datorā jau ielādēts pārvaldības aģents, ko izmanto gan risinājums HP Client Automation Standard, gan Enterprise Editions. Ja tas ir instalēts, tiek iespējota saziņa ar HP pārvaldības konsoli.

Lai instalētu HP programmatūras aģentu:

1. Noklikšķiniet uz **Start** (Sākt).
2. Noklikšķiniet uz **All Programs** (Visas programmas).
3. Noklikšķiniet uz **HP Manageability** (HP pārvaldāmība).
4. Noklikšķiniet uz **Radia Management Agent Readme** (Radia Management Agent lasimani).
5. Pārskatiet un ievērojiet failā Lasimani iekļautos norādījumus par HP Software Agent instalēšanu.

HP Software Agent ir galvenais infrastruktūras komponents, kas paredzēts visu HP Client Automation risinājumu iespējošanai. Lai iegūtu informāciju par citiem HP konfigurācijas pārvaldības risinājumiem, kas nepieciešami HP konfigurācijas pārvaldības risinājumu ieviešanai, apmeklējiet http://h20229.www2.hp.com/solutions/ascm/index.html.

Altiris Deployment Solution Agent

Šī programma ir sākotnēji ielādēta datorā. Ja tā ir instalēta, tiek nodrošināta saziņa ar administratora ieviešanas risinājumu konsoli.

Lai instalētu Altiris Deployment Solution Agent:

1. Noklikšķiniet uz **Start** (Sākt).
2. Noklikšķiniet uz **All Programs** (Visas programmas).
3. Noklikšķiniet uz **Install Altiris DAgent** (Instalēt Altiris DAgent) (sistēmā Windows Vista). Noklikšķiniet uz **Install Altiris AClient** (Instalēt Altiris AClient) (sistēmā Windows XP).
4. Izpildiet ekrānā redzamos norādījumus, lai uzstādītu un konfigurētu utilītu Altiris client.

Šis aģents ir galvenais infrastruktūras komponents, kas ļauj iespējot Altiris Deployment Solution — daļu no Altiris Client Management Suite. Lai iegūtu informāciju par citiem infrastruktūras komponentiem, kas nepieciešami Altiris Client Management Suite ieviešanai, apmeklējiet http://www.hp.com/go/easydeploy.

3 Attālā sistēmas instalēšana

Attālā sistēmas instalācija ļauj startēt un iestatīt sistēmu, izmantojot programmatūras un konfigurācijas informāciju, kas atrodas tīkla serverī, iniciējot pirmssāknēšanas izpildes vidi (PXE). Līdzeklis Attālā sistēmas instalācija parasti tiek izmantots kā sistēmas iestatīšanas un konfigurācijas rīks, un to var lietot šādiem uzdevumiem:

- Cietā diska formatēšanu
- Programmatūras attēla ieviešanu vienā vai vairākos datoros
- Attālu sistēmas BIOS jaunināšanu pārrakstāmajā ROM (Attālā ROM zibatmiņa 15. lpp.)
- Sistēmas BIOS iestatījumu konfigurēšanu

Lai startētu attālās sistēmas instalēšanas līdzekli, nospiediet taustiņu F12, kad, sāknējot datoru, ekrānā ar HP logotipu labajā apakšējā stūrī tiek parādīts paziņojums **F12 = Network Service Boot** (F12 = tīkla pakalpojuma sāknēšana). Lai turpinātu darbu, izpildiet ekrānā redzamos norādījumus. Noklusētā sāknēšanas secība ir BIOS konfigurācijas iestatījums, kuru var mainīt, lai iestatītu PXE sāknēšanu.

4 Programmatūras atjaunināšana un pārvaldība

HP piedāvā vairākus rīkus programmatūras atjaunināšanai un pārvaldībai galddatoros, darbstacijās un piezīmjdatoros:

- HP Client Management interfeiss
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Automation Starter, Standard un Enterprise Editions
- HP Client Manager no Symantec
- Altiris Client Management Suite
- HP Client Catalog, kas paredzēts Microsoft System Center & SMS Products
- HP Backup and Recovery Manager
- Intel vPro datori ar aktīvās pārvaldības tehnoloģiju
- Verdiem Surveyor
- HP Proactive Change Notification
- HP Subscriber's Choice

HP Client Management interfeiss

Neatkarīgi no sistēmas pārvaldības rīkiem, ko lieto jūsu IT nodaļa, ir svarīga gan aparatūras, gan programmatūras līdzekļu uzturēšana, lai nepaaugstinātos IT izmaksas un jūsu uzņēmums būtu elastīgs. IT administratori var piekļūt HP Client Management interfeisam, uzrakstot vienkāršus skriptus un integrējot tos izvēlētajos pārvaldības risinājumos.

Ar HP Client Management interfeisu (HP CMI) jaunie HP biznesa datori tiek vienlaidu integrēti pārvaldītajā IT vidē. HP CMI nodrošina interfeisu, kas vienkāršo HP biznesa datoru integrāciju ar populāriem nozares sistēmas pārvaldības rīkiem (iekļaujot Microsoft Systems Management Server, IBM Tivoli Software un HP Operations) un pielāgotām iekšēji izstrādātām pārvaldības lietojumprogrammām. Izmantojot HP CMI, sistēmas pārvaldības rīki un lietojumprogrammas var pieprasīt detalizētu klienta inventāru, saņemt veselības statusa informāciju un pārvaldīt sistēmas BIOS iestatījumus, veicot tiešu

komunikāciju ar klienta datoru, samazinot nepieciešamību pēc aģenta vai savienotāja programmatūras, lai panāktu integrāciju.

HP Client Management interfeisa pamatā ir nozares standarti, kur ietverts Microsoft Windows pārvaldības interfeiss (MS WMI), Web bāzēta uzņēmumu pārvaldība (WBEM), sistēmas pārvaldības BIOS (SMBIOS), kā arī uzlabotais konfigurācijas un barošanas bloka interfeiss (ACPI). HP CMI ir pamattehnoloģija, kas tiek izmantota HP Client Management risinājumos. Izmantojot HP CMI, HP jums piedāvā iespējas izvēlēties, kā pārvaldīt savus HP klientu datorus.

HP Client Management interfeiss, ja to izmanto kopā ar sistēmas pārvaldības programmatūru, var veikt šādas funkcijas:

- Pieprasīt detalizētu klienta inventarizācijas informāciju — tvert detalizētu informāciju par procesoriem, cietajiem diskiem, atmiņu, BIOS, draiveriem, ieskaitot sensoru informāciju (piemēram, ventilatora ātrumu, spriegumu un temperatūru).
- Saņemt veselības statusa informāciju — abonēt visdažādākos klienta aparatūras brīdinājumus (piemēram, par pārkaršanu, ventilatora apstāšanos un aparatūras konfigurācijas izmaiņām), lai tie tiktu nosūtīti sistēmas pārvaldības konsolei, lietojumprogrammai vai lokālā klienta datoram. Brīdinājumi tiek nosūtīti reāllaikā, kad nostrādā aparatūras notikuma trigeris.
- Pārvaldīt sistēmas BIOS iestatījumus — veikt F10 funkcijas, ieskaitot BIOS paroles iestatīšanu un mainīšanu, kā arī uzsākt datora sāknēšanu attāli no sistēmas pārvaldības konsoles jebkurā vai visās klienta sistēmās bez nepieciešamības apmeklēt katru datoru.

Lai iegūtu papildinformāciju par HP Client Management interfeisu, skatiet http://www.hp.com/go/hpcmi/.

HP SoftPaq Download Manager

HP SoftPaq Download Manager ir bezmaksas, vienkārši izmantojams interfeiss HP klientu datoru modeļu programmatūras atjauninājumu atrašanai un lejupielādei savā vidē. Norādot modeļus, operētājsistēmu un valodu, varat ātri atrast, sakārtot un atlasīt nepieciešamās programmatūras pakotnes. Lai lejupielādētu HP SoftPaq Download Manager, apmeklējiet http://www.hp.com/go/sdm.

HP System Software Manager

HP System Software Manager (SSM) ir bezmaksas utilīta, kas automatizē ierīču draiveru un BIOS jauninājumu attālo ieviešanu jūsu HP biznesa datoros, kas ir pieslēgti tīklam. SSM bez lietotāja iejaukšanās nosaka pārbaudes līmeņus katra tīkla klienta sistēmā instalētajiem draiveriem un BIOS, salīdzina iegūtos rezultātus ar sistēmas programmatūras SoftPaqs palīdzību, kas ir testēta un saglabāta centrālajā failu krātuvē. Pēc tam SSM automātiski atjaunina visu pārbaudīto tīkla datoru sistēmu programmatūru uz jaunāko failu krātuvē atrodamo līmeni. Tā kā SSM ļauj SoftPaq jauninājumu izplatīšanu tikai pareiziem klientu sistēmu modeļiem, administratori var izmantot SSM konfidenciāli un efektīvi, lai uzturētu sistēmas programmatūras jauninājumu līmeni.

Programma System Software Manager ir integrējama ar uzņēmuma programmatūras izplatīšanas rīkiem, piemēram, HP Client Automation solutions, HP Client Manager from Symantec un Microsoft Systems Management Server (SMS). Izmantojot SSM, jūs varat izplatīt klientu izveidotos vai trešo pušu atjauninājumus, kas ir iepakoti SSM formātā.

SSM var lejupielādēt bez maksas, apmeklējot http://www.hp.com/go/ssm.

PIEZĪME SSM pašlaik neatbalsta attālu ROM pārrakstīšanu sistēmās, kurās ir iespējots Windows Vista BitLocker un tiek izmantotas TPM mērvienības, lai aizsargātu BitLocker atslēgas, jo BIOS mirgošana varētu bojāt uzticības parakstu, kuru BitLocker ir izveidojis šai platformai. Grupu politikā atspējojiet BitLocker, lai pārrakstītu sistēmu BIOS.

Lai nesabojātu BitLocker atslēgas, varat iespējot BitLocker atbalstu, neizmantojot BIOS TPM mērvienības. HP iesaka izveidot drošu BitLocker akreditācijas datu dublējumkopiju gadījumam, ja nepieciešams veikt ārkārtas atkopšanu.

HP ProtectTools Security Manager

HP ProtectTools Security Manager programmatūra sniedz drošības līdzekļus, kas aizsargā pret nepilnvarotu piekļuvi datoram, tīklam un kritiskiem datiem. Uzlaboto drošības funkcionalitāti sniedz šādi programmatūras moduļi:

- Credential Manager for HP ProtectTools
- Embedded Security for HP ProtectTools
- Java Card Security for HP ProtectTools
- BIOS Configuration for HP ProtectTools
- Drive Encryption for HP ProtectTools
- Device Access Manager for HP ProtectTools
- File Sanitizer, kas paredzēts HP ProtectTools
- Privacy Manager, kas paredzēts HP ProtectTools

Datoram pieejamie programmatūras moduļi var būt atkarīgi no jūsu datora modeļa. Piemēram, Embedded Security for HP ProtectTools ir pieejams tikai datoriem, kuros ir instalēta uzticamā platformas moduļa (TPM) iebūvētā drošības mikroshēma.

HP ProtectTools programmatūras moduļi var būt jau instalēti, jau ielādēti vai pieejami lejupielādei HP vietnē. Atsevišķām HP Compaq darbvirsmām HP ProtectTools ir pieejama kā pēcpārdošanas iespēja. Papildinformāciju skatiet http://www.hp.com/products/security.

HP Client Automation Starter un Standard Editions

HP Client Automation ir viegli lietojams un ātri izvietojams aparatūras un programmatūras pārvaldības risinājums sistēmai Windows Vista, Windows XP un HP Thin Client videi, kas nodrošina stabilus pamatus nākotnes prasībām. Tas tiek piedāvāts divos izdevumos:

- Starter Edition ir bezmaksas produkts, kas paredzēts HP galddatoru, piezīmjdatoru un darbstaciju pārvaldībai, nodrošinot aparatūras un programmatūras inventāru, attālo vadību, HP brīdinājumu pārraudzību, HP BIOS un diskdziņu atjauninājumus, HP Protect aizsardzības līdzekļu integrēšanu un Intel AMT pievienojumprogrammu atbalstu. Starter Edition arī atbalsta līdzekļa HP Thin Clients izvietošanu un pārvaldību.
- Standard Edition, ko var iegādāties par samaksu, ietver visu Starter Edition funkcionalitāti. Papildus tajā ir iekļautas pievienojumprogrammas Windows izvietošanai un migrēšanai, ielāpu pārvaldības iespējas, programmatūras izplatīšana un programmatūras mērīšanas izmantošana.

HP Client Automation Starter un Standard Editions nodrošina migrēšanas ceļu uz HP Client Automation Enterprise Edition (pamatā Radia tehnoloģija), lai varētu automātiski pārvaldīt lielas, neviendabīgas un nemitīgi mainīgas IT vides.

Papildinformāciju par HP Client Automation risinājumiem skatiet http://www.hp.com/go/client.

HP Client Automation Enterprise Edition

HP Client Automation Enterprise Edition ir uz politikām balstīts risinājums, kas ļauj administratoriem veikt inventarizāciju, izvietošanu, ielāpu izveidi un nepārtrauktu programmatūras un satura pārvaldīšanu vairākās neviendabīgās klienta platformās. Izmantojot HP Client Automation Enterprise Edition, IT profesionāļi var:

- Automatizēt visa dzīves cikla pārvaldību, sākot no atklāšanas, izvietošanas, pārraudzības un beidzot ar migrēšanu un norakstīšanu
- Automātiski izvietot un nepārtraukti pārvaldīt visu programmatūras steku (operētājsistēmas, lietojumprogrammas, ielāpus, iestatījumus un saturu) sev vēlamajā līmenī
- Virtuāli pārvaldīt programmatūru jebkurā ierīcē, ieskaitot galddatoros, darbstacijās, klēpjdators gan neviendabīgā, gan savrupā infrastruktūrā
- Pārvaldīt programmatūru lielākajā daļā operētājsistēmu

Lietojot nepārtrauktu konfigurācijas pārvaldību, HP klienti ziņo, ka ievērojami samazinās IT izmaksas, tādējādi samazinot programmatūras un satura iekļaušanai tirgū nepieciešamo laiku, kā arī uzlabojot lietotāju produktivitāti un apmierinātību.

Papildinformāciju par HP Client Automation risinājumiem skatiet http://www.hp.com/go/client.

HP Client Manager no Symantec

HP Client Manager no Symantec, izstrādāts ar Altiris, ir pieejams bez maksas visiem atbalstītajiem HP biznesa galddatoru, piezīmjdatoru un darbstaciju modeļiem. SSM ir integrēts HP Client Manager un iespējo centrālo izsekošanu, pārraudzību un HP klienta sistēmu aparatūras aspektu pārvaldību.

Izmantojiet HP Client Manager no Symantec, lai:

- Iegūtu vērtīgu informāciju par aparatūru, piemēram, CPU, atmiņas, video un drošības iestatījumus
- Pārraudzītu sistēmas stāvokli un atrisinātu problēmas, pirms tās ir radušās
- Automātiski iegūtu un instalētu BIOS atjauninājumus, neapmeklējot katru datoru
- Attāli konfigurētu BIOS un drošības iestatījumus
- Automatizētu aparatūras problēmu ātrās risināšanas procesu

Cieša integrācija ar HP Instant Support rīkiem samazina aparatūras problēmu novēršanas laiku

- Diagnostika — ļauj attāli izpildīt un skatīt atskaites par HP galddatoru, piezīmjdatoru vai darbstaciju modeļiem
- Sistēmas veselības skenēšana — ļauj pārbaudīt, vai jūsu uzstādītajā HP klientu sistēmu bāzē nav zināmo aparatūras problēmu
- Aktīva tērzēšana — ļauj sazināties ar HP klientu atbalsta darbiniekiem, lai novērstu problēmas
- HP zināšanu bāzes — nodrošina saiti uz ekspertinformāciju
- Automatizētais SoftPaq savākšanas un piegādes process ātri novērš aparatūras problēmas
- Izmantojot HP ProtectTools iebūvēto drošības mikroshēmu, tiek identificētas, inventarizētas un inicializētas sistēmas
- Ir iespēja veselības brīdinājumus parādīt lokāli klienta sistēmā
- Ir iespēja veidot atskaites par inventarizācijas pamatinformāciju klientiem, kas nav HP klienti
- Iestatīt un konfigurēt TPM drošības mikroshēmu
- Centralizēti ieplānot HP Client dublēšanu un atkopšanu
- Saņemt atbalstu Intel AMT pārvaldīšanai

Papildinformāciju par HP Client Manager no Symantec skatiet http://www.hp.com/go/clientmanager.

Altiris Client Management Suite

Altiris Client Management Suite ir viegli izmantojams risinājums pilnīgai galddatoru, piezīmjdatoru un darbstaciju dzīves cikla pārvaldībai. Client Management Suite Level 1 ietver šādus Altiris produktus:

- Inventory solution
- Deployment Solution
- Software Delivery Solution
- Patch Management Solution
- Application Metering Solution
- Application Management Solution
- Carbon Copy Solution

Papildinformāciju par Altiris Client Management Suite skatiet http://www.altiris.com/Products/ClientManagementSuite.aspx.

HP Client Catalog, kas paredzēts Microsoft System Center & SMS Products

HP Client Catalog ļauj IT profesionāļiem, kas izmanto Microsoft produktus, automatizēt HP programmatūras atjauninājumu (programmatūras pakotņu) ieviešanu HP biznesa datoriem. Kataloga failā ir iekļauta detalizēta platformas informācija par HP biznesa galddatoriem, piezīmjdatoriem un darbstacijām. To var izmantot saistībā ar pielāgoto inventāru un Microsoft produktu atjaunināšanas līdzekļiem, lai nodrošinātu automatizētus draivera un ielāpu atjauninājumus pārvaldītiem HP klientu datoriem.

Pie Microsoft produktiem, ko atbalsta HP Client Catalog, pieder:

- System Center Configuration Manager 2007
- System Center Essentials 2007
- Systems Management Server (SMS) 2003 R2

Papildinformāciju par HP Client SMS katalogu skatiet http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html.

HP Backup and Recovery Manager

HP Backup and Recovery Manager ir viegli izmantojama dažādiem mērķiem paredzēta lietojumprogramma, kas datorā nodrošina cietā diska sākotnējā stāvokļa dublēšanu un atkopšanu. Šī lietojumprogramma darbojas sistēmā Windows un izveido Windows, visu lietojumprogrammu un datu failu dublējumkopijas. Dublējumkopiju izveidi var ieplānot automātiski, norādot intervālus, vai veikt manuāli. Svarīgus failus var arhivēt atsevišķi ārpus plānotajām dublējumkopiju izveidēm.

HP Backup and Recovery Manager ir sākotnēji instalēts C: diskdzinī un veido atkopšanas nodalījumu.

Atkopšanas punktus un failu dublējumkopijas var kopēt kompaktdiskos vai DVD diskos, savukārt visas dublējumkopijas var kopēt tīklā vai sekundārajos cietajos diskos.

HP iesaka izveidot diska atkopšanas komplektu vēl pirms datora izmantošanas un ieplānot regulāru automātisko atkopšanas punktu izveidi.

Lai izveidotu diska atkopšanas komplektu:

1. Noklikšķiniet uz **Start** (Sākt) > **HP Backup and Recovery** > **HP Backup and Recovery Manager**, lai atvērtu dublējumkopiju izveides un atkopšanas vedni, pēc tam noklikšķiniet uz **Next** (Tālāk).
2. Atlasiet **Create a set of recovery discs (Recommended)** (Izveidot diska atkopšanas komplektu (Ieteicams)) un noklikšķiniet uz **Next** (Tālāk).
3. Izpildiet vedņa instrukcijas.

Papildinformāciju par HP Backup and Recovery Manager izmantošanu skatiet *HP Backup and Recovery Manager rokasgrāmatā*, ko varat atrast, atlasot **Start** (Sākt) > **HP Backup and Recovery** > **HP Backup and Recovery Manager Manual**.

PIEZĪME Diska atkopšanas komplektu var pasūtīt, sazinoties ar HP atbalsta dienestu. Dodieties uz šo Web vietu, atlasiet savu reģionu un sadaļā **Call HP** (Sazināties ar HP) noklikšķiniet uz saites **Technical support after you buy** (Tehniskais atbalsts pēc produkta iegādes), lai uzzinātu tehniskā atbalsta centra tālruņa numuru savā reģionā.

http://welcome.hp.com/country/us/en/wwcontact_us.html

Pārvaldības tehnoloģija

Modeļi iekļauj vPro tehnoloģiju vai standarta tehnoloģiju. Tās abas ļauj labāk atklāt, izlabot un aizsargāt tīkla aprēķinus. Abas tehnoloģijas ļauj pārvaldīt datorus, kad sistēma ir ieslēgta vai izslēgta vai arī operētājsistēma ir uzkārusies.

Pārvaldības tehnoloģijas līdzekļi:

- Aparatūras inventarizācijas informācija
- Brīdinājumi
- Enerģijas pārvaldība — ieslēgšana/izslēgšana, cikla enerģija
- Attālā diagnosticēšana un labošana
    - Tehnoloģija Serial Over LAN — tas nodrošina attālu datoru kontroli sāknēšanas laikā, izmantojot konsoli
    - IDE virzienmaiņa — tā atļauj sistēmas sāknēšanu no attāla sāknēšanas diska vai ISO attēla
- Izolēšana un atkopšana aparatūras līmenī — tas ļauj ierobežot vai atslēgt datora tīkla piekļuvi, ja konstatētas vīrusiem atbilstošas darbības

PIEZĪME Lai iegūtu pārskatu par Intel vPro tehnoloģiju, apmeklējiet http://www.intel.com/vpro.

HP izstrādājumiem atbilstošo informāciju par Intel vPro tehnoloģiju skatiet publiskajā aprakstā http://www.hp.com/support. Izvēlieties valsti un valodu, atlasiet **See support and troubleshooting information** (Apskatīt informāciju par atbalstu un problēmu novēršanu), ievadiet datora modeļa numuru un nospiediet taustiņu Enter. Kategorijā **Resources** (Resursi) noklikšķiniet uz **Manuals** (guides, supplements, addendums, etc) (Rokasgrāmatas (norādījumi, papildinājumi, pielikumi u.c.)). Sadaļā **Quick jump to manuals by category** (Ātra pāriešana pie rokasgrāmatām pēc kategorijas) noklikšķiniet uz **White papers** (Baltie papīri).

Pieejamās pārvaldības tehnoloģijas:

- AMT (iekļauj DASH 1.0)
- ASF

ASF un AMT vienlaikus nevar konfigurēt, bet abas tiek atbalstītas.

Lai Intel vPro sistēmas konfigurētu AMT vai ASF izmantošanai:

1. Ieslēdziet vai restartējiet datoru. Operētājsistēmā Microsoft Windows noklikšķiniet uz **Start** (Sākt) > **Shut Down** (Beidzēt) > **Restart** (Restartēt).
2. Tūlīt pēc datora ieslēgšanas nospiediet karsto taustiņu, taustiņu kombināciju Ctrl+P, pirms dators sāknē operētājsistēmu.

    PIEZĪME Ja taustiņu kombinācija Ctrl+P netiek nospiesta atbilstošajā brīdī, restartējiet datoru un vēlreiz nospiediet taustiņu kombināciju Ctrl+P, pirms dators sāknē operētājsistēmu, lai piekļūtu utilītai.

Šī karsto taustiņu kombinācija atver uzstādīšanas utilītu Intel Management Engine BIOS Execution (MEBx). Šī utilīta lietotājam ļauj konfigurēt dažādus pārvaldības tehnoloģijas aspektus. Tālāk ir norādītas dažas no konfigurācijas opcijām:

- Galvenā izvēlne
  - Intel ® ME konfigurācija
  - Intel ® AMT konfigurācija
  - Intel ® ME paroles maiņa
  - Exit (Iziet)
- Intel ® ME platformas konfigurācija
  - Intel ® ME stāvokļa vadība (iespējot/atspējot)
  - Intel ® ME programmaparatūras lokālā atjaunināšana (iespējot/atspējot)
  - Intel ® ME līdzekļu vadība
  - Intel ® ME strāvas vadība
- Intel ® AMT konfigurācija
  - Resursdatora nosaukums
  - TCP/IP
  - Apgādes modelis (uzņēmums, SMB)
  - Uzstādīšana un konfigurācija
  - Antiapgāde
  - SOL/IDE-R (iespējot/atspējot)
  - Paroles politika
  - Droša programmaparatūras atjaunināšana (iespējot/atspējot)
  - Iestatīt PRTC
  - Dīkstāves taimauts
- Intel ® ME paroles maiņa (HP ļoti iesaka nomainīt šo paroli. Noklusējuma parole ir **admin**.)

Lai attālināti pārvaldītu AMT sistēmas, administratoram jāizmanto attālā konsole, kas atbalsta AMT. Dažādi izstrādātāji piedāvā uzņēmumu pārvaldības konsoles, piemēram, HP Altiris un Microsoft SMS. SMB režīmā klients nodrošina Web pārlūkprogrammas interfeisu. Lai piekļūtu šim līdzeklim, atveriet pārlūkprogrammu no jebkuras citas tīklā esošas sistēmas un ievadiet `http://resursdatora_nosaukums:16992`, kur `resursdatora_nosaukums` ir sistēmai piešķirtais nosaukums. Vai arī resursdatora nosaukuma vietā izmantojiet IP adresi.

Verdiem Surveyor

Verdiem Surveyor ir programmatūras risinājums, kas palīdz pārvaldīt datora enerģijas izmaksas. Surveyor izmēra un paziņo, cik enerģijas patērē katrs dators. Tas arī nodrošina datora barošanas iestatījumus, ļaujot administratoriem viegli izmantot tīklos enerģijas taupīšanas stratēģiju. HP SoftPaq, kurā ir Surveyor agent, var lejupielādēt no HP atbalsta Web vietas un instalēt atbalstītos komerciālo galddatoru modeļos. Surveyor licences pārvaldības datoriem var iegādāties ar HP pārstāvja palīdzību.

HP Proactive Change Notification

Programma Proactive Change Notification lieto Web vietu Subscriber's Choice, lai proaktīvi un automātiski:

- Līdz pat 60 dienām iepriekš nosūtītu e-pasta ziņojumus Proactive Change Notification (PCN – Aktīvā paziņošana par izmaiņām) par aparatūras un programmatūras izmaiņām lielākajai komerciālo datoru un serveru daļai
- Nosūtītu e-pasta ziņojumu, kurā ietverti informatīvie materiāli Customer Bulletins, Customer Advisories, Customer Notes, Security Bulletins un ar draiveru problēmām saistīti brīdinājumi lielākajai daļai komerciālo datoru un serveru

Izveidojiet pielāgotu profilu, lai nodrošinātu tikai noteiktai IT videi atbilstošas informācijas saņemšanu. Lai iegūtu plašāku informāciju par programmu Proactive Change Notification un izveidotu pielāgotu profilu, apmeklējiet http://h30046.www3.hp.com/subhub.php

Subscriber's Choice

Subscriber's Choice ir klientiem paredzēts HP pakalpojums.

Atbilstoši lietotāja izveidotajam profilam HP nosūta individuālus padomus par produktiem, informāciju par līdzekļiem un/vai draiveru un atbalsta brīdinājumus/paziņojumus.

Izmantojot pakalpojuma Subscriber’s Choice (Abonentu izvēle) draiveri un atbalsta brīdinājumus vai paziņojumus, tiek nosūtīti e-pasta ziņojumi, lai informētu par iespēju pārskatīt un atgūt savā profilā abonēto informāciju. Lai uzzinātu vairāk par pakalpojumu Subscriber’s Choice un izveidotu pielāgotu profilu, apmeklējiet http://h30046.www3.hp.com/subhub.php.

Risinājumi, kas netiek tālāk attīstīti

Divas programmatūras pakotnes (Altiris Local Recovery un Dantz Retrospect) vairs netiek iekļautas HP biznesa galddatoru, piezīmjdatoru un darbstaciju komplektācijā. Sākot ar 2006. gadu, jaunie biznesa galddatori, piezīmjdatori un darbstacijas tiek komplektētas ar HP Backup and Recovery Manager.

5 ROM Flash

Datora BIOS tiek glabāta programmējamā zibatmiņā ROM (lasāmatmiņā). Norādot iestatījumu paroli, izmantojot utilītu Computer Setup (F10), lasāmatmiņu var aizsargāt pret netīšu jaunināšanu vai pārrakstīšanu. Tā ir nepieciešama, lai nodrošinātu datora darbības integritāti. Ja ir jāveic BIOS jaunināšana, jaunākos BIOS attēlus var lejupielādēt HP draiveru un atbalsta lapā http://www.hp.com/support/files.

△ **UZMANĪBU!** Lai gūtu maksimālu ROM aizsardzību, norādiet iestatījumu paroli. Iestatījumu parole novērš nesankcionētu ROM jaunināšanu. Utilīta System Software Manager ļauj sistēmas administratoram iestatīt iestatījumu paroli vienā vai vairākos datoros vienlaicīgi. Papildinformāciju skatiet http://www.hp.com/go/ssm.

Attālā ROM zibatmiņa

Programma Remote ROM Flash ļauj sistēmas administratoram droši jaunināt attālu HP datoru BIOS tieši no centralizētās tīkla vadības konsoles. Tas sistēmas administratoram ļauj veikt šo uzdevumu attālināti vairākos datoros tīklā, tā konsekventi veicot HP datoru BIOS attēlu ieviešanu un efektīvāku pārvaldīšanu. Šādi tiek panākta arī augstāka produktivitāte un samazinātas kopējās izmaksas.

PIEZĪME SSM pašlaik neatbalsta attālu ROM pārrakstīšanu sistēmās, kurās ir iespējots Windows Vista BitLocker un tiek izmantotas TPM mērvienības, lai aizsargātu BitLocker atslēgas, jo BIOS mirgošana varētu bojāt uzticības parakstu, kuru BitLocker ir izveidojis šai platformai. Grupu politikā atspējojiet BitLocker, lai pārrakstītu sistēmu BIOS.

Lai izmantotu priekšrocības, datoram jābūt pieslēgtam pie strāvas vai ieslēgtam, izmantojot Remote Wakeup.

Plašāku informāciju par Remote ROM Flash skatiet sadaļā HP Client Manager Software vai System Software Manager, apmeklējot http://www.hp.com/go/ssm/.

HPQFlash

Utilīta HPQFlash tiek lietota, lai lokāli jauninātu vai atjaunotu atsevišķu datoru BIOS, izmantojot operētājsistēmu Windows.

Papildinformāciju par utilītu HPQFlash skatiet http://www.hp.com/support/files un pēc uzaicinājuma ievadiet datora modeļa numuru.

6 Sāknēšanas bloķēšanas avārijas atkopšanas režīms

Sāknēšanas bloķēšanas avārijas atkopšanas režīms ļauj veikt sistēmas atkopšanu tajā praktiski neiespējamajā gadījumā, ja rodas ROM pārrakstīšanas kļūme. Piemēram, ja BIOS jaunināšanas laikā rodas enerģijas piegādes traucējumi, ROM pārrakstīšana netiek pabeigta. Tas sistēmu BIOS padarītu nelietojamu. Sāknēšanas bloks ir pret pārrakstīšanu aizsargāta ROM atmiņas daļa, kas, ieslēdzot sistēmu, meklē derīgu BIOS zibatmiņas kopiju.

- Ja sistēmas BIOS attēls ir derīgs, sistēma tiek startēta kā parasti.
- Ja sistēmas BIOS attēls nav derīgs, atteikumdroša sāknēšanas bloka BIOS nodrošina pietiekamu atbalstu, lai meklētu noņemamu BIOS attēla failu datu nesēju. Ja ir atrasts atbilstošs BIOS attēla fails, tas tiek automātiski ierakstīts atmiņā ROM.

Ja tiek atklāts nederīgs sistēmas BIOS attēls, sistēmas strāvas indikators reizi sekundē 8 reizes mirgo sarkanā krāsā. Vienlaikus skaļrunis 8 reizes atskaņo skaņas signālu. Ja tā sistēmas ROM daļa, kurā iekļauts video opcijas ROM attēls, nav bojāta, ekrānā tiek rādīts ziņojums **Boot Block Emergency Recovery Mode** (Sāknēšanas bloka avārijas atkopšanas režīms).

Lai atkoptu sistēmu pēc tās ieiešanas sāknēšanas bloka avārijas atkopšanas režīmā, veiciet šādas darbības:

1. Izslēdziet datoru.
2. Ievietojiet kompaktdisku vai USB zibatmiņas ierīci ar saknes direktorijā saglabātu nepieciešamo BIOS attēla failu.

   PIEZĪME Datu nesējam jābūt formatētam, izmantojot failu sistēmu FAT12, FAT16 vai FAT32.

3. Ieslēdziet datoru.

   Ja ir atrasts atbilstošs BIOS attēls, jums lūgs ievietot datu nesēju ar BIOS attēla failu.

   Ja sistēma sekmīgi pārprogrammē atmiņu ROM, sistēma automātiski izslēdzas.

4. Izņemiet noņemamo datu nesēju, kas izmantots BIOS jaunināšanai.
5. Ieslēdziet datoru, lai to restartētu.

PIEZĪME BitLocker aizkavē Windows Vista no sāknēšanas, kad optiskajā diskā ir ievietots kompaktdisks ar BIOS attēla failu. Ja ir iespējots BitLocker, noņemiet šo kompaktdisku pirms mēģinājuma sāknēt Windows Vista.

7 Iestatījumu replicēšana

Ar šo procedūru administrators var viegli iekopēt datora iestatījumu konfigurāciju citos tāda paša modeļa datoros. Šādi var ātrāk un saskaņotāk veikt vairāku datoru konfigurāciju.

PIEZĪME Abām procedūrām ir nepieciešams diskešu diskdzinis vai atbalstītais USB zibatmiņas disks.

Kopēšana vienā datorā

△ **UZMANĪBU!** Iestatījumu konfigurācija ir atkarīga no datora modeļa. Ja datora, no kura tiek veikta kopēšana, modelis nav vienāds ar tā datora modeli, kurā jākopē, var rasties failu sistēmas bojājums. Piemēram, nekopējiet dc7xxx datora iestatījumu konfigurāciju dx7xxx datorā.

1. Atlasiet iestatījumu konfigurāciju, kas jākopē. Izslēdziet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start** (Sākt) > **Shut Down** (Beidzēt) > **Shut Down** (Beidzēšana).
2. Ja lietojat USB zibatmiņas datu nesēju, ievietojiet to.
3. Ieslēdziet datoru.
4. Tūlīt pēc datora ieslēgšanas nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai ieietu datora uzstādīšanā. Nospiediet taustiņu Enter, lai apietu nosaukumlapu, ja tas ir nepieciešams.

   PIEZĪME Ja taustiņš F10 netiek nospiests atbilstošajā brīdī, restartējiet datoru un vēlreiz nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai piekļūtu utilītai.
5. Ja lietojat disketi, ievietojiet to.
6. Noklikšķiniet uz **File** (Fails) > **Replicated Setup** (Replicētie iestatījumi) > **Save to Removable Media** (Saglabāt noņemamā datu vidē). Lai izveidotu konfigurēšanas disketi vai USB zibatmiņas datu nesēju, izpildiet ekrānā redzamos norādījumus.
7. Izslēdziet datoru, kuru vēlaties konfigurēt, un ievietojiet konfigurēšanas disketi vai USB zibatmiņas datu nesēju.
8. Ieslēdziet datoru, kas jākonfigurē.
9. Tūlīt pēc datora ieslēgšanas nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai ieietu datora uzstādīšanā. Nospiediet taustiņu Enter, lai apietu nosaukumlapu, ja tas ir nepieciešams.
10. Noklikšķiniet uz **File** (Fails) > **Replicated Setup** (Replicēti iestatījumi) > **Restore from Removable Media** (Atjaunot no noņemamas datu vides) un izpildiet ekrānā redzamos norādījumus.
11. Kad konfigurēšana ir pabeigta, restartējiet datoru.

Kopēšana vairākos datoros

△ **UZMANĪBU!** Iestatījumu konfigurācija ir atkarīga no datora modeļa. Ja datora, no kura tiek veikta kopēšana, modelis nav vienāds ar tā datora modeli, kurā jākopē, var rasties failu sistēmas bojājums. Piemēram, nekopējiet dc7xxx datora iestatījumu konfigurāciju dx7xxx datorā.

Lai sagatavotu konfigurēšanas disketi vai USB zibatmiņas datu nesēju atbilstoši šai metodei, nepieciešams nedaudz vairāk laika, taču konfigurācija tiek iekopēta mērķdatoros ievērojami ātrāk.

PIEZĪME Lai veiktu šo procedūru, ir nepieciešama sāknēšanas diskete vai izveidots USB zibatmiņas datu nesējs, ar kuru var veikt sāknēšanu. Ja sāknēšanas disketes izveidošanai nav pieejama operētājsistēma Windows XP, veiciet darbības, kas paredzētas kopēšanai vienā datorā (sk. Kopēšana vienā datorā 17. lpp.).

1. Izveidojiet sāknēšanas disketi vai USB zibatmiņas datu nesēju. Sk. Atbalstītā USB zibatmiņas datu nesēja ierīce 19. lpp. vai Neatbalstītā USB zibatmiņas datu nesēja ierīce 20. lpp. .

   △ **UZMANĪBU!** Visus datorus nevar sāknēt no USB zibatmiņas datu nesēja. Ja utilītas Computer Setup (F10) noklusētajā sāknēšanas secības sarakstā USB ierīce ir norādīta pirms cietā diska, datoru var sāknēt no USB zibatmiņas datu nesēja. Pretējā gadījumā jālieto sāknēšanas diskete.

2. Atlasiet iestatījumu konfigurāciju, kas jākopē. Izslēdziet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start** (Sākt) > **Shut Down** (Beidzēt) > **Shut Down** (Beidzēšana).

3. Ja lietojat USB zibatmiņas datu nesēju, ievietojiet to.

4. Ieslēdziet datoru.

5. Tūlīt pēc datora ieslēgšanas nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai ieietu datora uzstādīšanā. Nospiediet taustiņu Enter, lai apietu nosaukumlapu, ja tas ir nepieciešams.

   PIEZĪME Ja taustiņš F10 netiek nospiests atbilstošajā brīdī, restartējiet datoru un vēlreiz nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai piekļūtu utilītai.

6. Ja lietojat disketi, ievietojiet to.

7. Noklikšķiniet uz **File** (Fails) > **Replicated Setup** (Replicētie iestatījumi) > **Save to Removable Media** (Saglabāt noņemamā datu vidē). Lai izveidotu konfigurēšanas disketi vai USB zibatmiņas datu nesēju, izpildiet ekrānā redzamos norādījumus.

8. Lai replicētu iestatījumus, lejupielādējiet utilītu BIOS (repset.exe) un iekopējiet to konfigurēšanas disketē vai USB zibatmiņas datu nesējā. Lai iegūtu šo utilītu, dodieties uz http://welcome.hp.com/country/us/en/support.html un ievadiet datora modeļa numuru.

9. Konfigurēšanas disketē vai USB zibatmiņas datu nesējā izveidojiet failu autoexec.bat, kas ietver šādu komandu:

   ```
   repset.exe
   ```

10. Izslēdziet konfigurējamo datoru. Ievietojiet konfigurēšanas disketi vai USB zibatmiņas datu nesēju un ieslēdziet datoru. Automātiski tiek palaista konfigurēšanas utilīta.

11. Kad konfigurēšana ir pabeigta, restartējiet datoru.

Sāknējamas ierīces izveidošana

Atbalstītā USB zibatmiņas datu nesēja ierīce

Atbalstītajām ierīcēm ir sākotnēji instalēts attēls, kas vienkāršo to padarīšanu par sāknējamām. Visām HP un Compaq, kā arī vairākumam citu USB zibatmiņas datu nesēju ierīcēm ir šāds sākotnēji instalēts attēls. Ja izmantotajam USB zibatmiņas datu nesējam nav šī attēla, veiciet šajā nodaļā tālāk norādītās darbības (sk. Neatbalstītā USB zibatmiņas datu nesēja ierīce 20. lpp.).

Lai izveidotu sāknēšanas USB zibatmiņas datu nesēju, jābūt:

- Atbalstītai USB zibatmiņas iekārtai
- Sāknējamai DOS disketei ar FDISK vai SYS programmām (ja programma SYS nav pieejama, var lietot programmu FORMAT, taču tādā gadījumā tiks zaudēti visi USB zibatmiņas datu nesēja faili)
- Datoram, kuru var sāknēt no USB zibatmiņas iekārtas

△ **UZMANĪBU!** Dažus vecākus datorus var neizdoties sāknēt no USB zibatmiņas iekārtas. Ja utilītas Computer Setup (F10) noklusētajā sāknēšanas secības sarakstā USB ierīce ir norādīta pirms cietā diska, datoru var sāknēt no USB zibatmiņas datu nesēja. Pretējā gadījumā jālieto sāknēšanas diskete.

1. Izslēdziet datoru.
2. Ievietojiet USB zibatmiņas datu nesēju kādā no datora USB portiem un noņemiet visas pārējās USB atmiņas ierīces, izņemot USB diskešu diskdziņus.
3. Ievietojiet diskešu diskdzinī sāknēšanas DOS disketi, kurā ietvertas programmas FDISK.COM un SYS.COM vai FORMAT.COM, pēc tam ieslēdziet datoru, lai veiktu sāknēšanu uz DOS disketi.
4. Palaidiet FDISK no **A:** uzvednes, ierakstot `FDISK` un nospiežot Enter. Pēc uzvednes parādīšanas noklikšķiniet uz **Yes** (Jā) (**Y**), lai iespējotu lielo diska atbalstu.
5. Ievadiet Choice [`5`], lai parādītu sistēmā esošos diskdziņus. USB zibatmiņas datu nesējs būs tas diskdzinis, kura lielums līdzinās kādam no sarakstā norādītājiem diskdziņiem. Parasti tas ir pēdējais saraksta diskdzinis. Pierakstiet diskdziņa burtu.

   USB zibatmiņas datu nesēja diskdzinis: _____

   △ **UZMANĪBU!** Ja diskdzinis neatbilst USB zibatmiņas datu nesējam, neturpiniet darbības. Pretējā gadījumā varat zaudēt datus. Pārbaudiet, vai kādā no USB portiem nav papildu atmiņas ierīču. Ja atrodat atmiņas ierīces, noņemiet tās, vēlreiz sāknējiet datoru un turpiniet, sākot no 4. darbības. Ja ierīces netiek atrastas, iespējams, sistēma neatbalsta USB zibatmiņas datu nesēju vai USB zibatmiņas datu nesējs ir bojāts. NETURPINIET USB zibatmiņas datu nesēja pārveidošanu par sāknēšanas ierīci.
6. Izejiet no programmas FDISK, nospiežot taustiņu Esc, tādējādi atgriežoties uzvednē **A:**.
7. Ja DOS sāknēšanas disketē ietverta programma SYS.COM, pārejiet uz 8. darbību. Pretējā gadījumā pārejiet uz 9. darbību.
8. Uzvednē **A:** ievadiet `SYS x:`, x vietā norādot iepriekš pierakstīto burtu.

   △ **UZMANĪBU!** Ievadiet USB zibatmiņas datu nesējam atbilstošo diska burtu.

   Kad sistēmas faili ir pārsūtīti, programma SYS atgriežas uzvednē **A:**. Pārejiet uz 13. darbību.

9. USB zibatmiņas datu nesēja failus, kurus vēlaties paturēt, iekopējiet cita diska (piemēram, sistēmas iekšējā cietā diska) pagaidu direktorijā.

10. Uzvednē **A:** ievadiet `FORMAT /S X:`, `X` vietā norādot iepriekš pierakstīto burtu.

△ **UZMANĪBU!** Ievadiet USB zibatmiņas datu nesējam atbilstošo diska burtu.

FORMAT parādīs vienu vai vairākus ziņojumus un katru reizi vaicās, vai vēlaties turpināt. Katru reizi ievadiet `Y`. FORMAT formatēs USB zibatmiņas datu nesēja ierīci, pievienos sistēmas failus un vaicās par sējuma etiķeti.

11. Nospiediet taustiņu Enter, ja nevēlaties ievadīt etiķeti, vai ievadiet to, ja vēlaties.

12. Kopējiet 9. darbībā saglabātos failus atpakaļ USB zibatmiņas datu nesējā.

13. Izņemiet disketi un no jauna sāknējiet datoru. Dators veiks sāknēšanu uz USB zibatmiņas datu nesēju kā uz C disku.

PIEZĪME Noklusētā sāknēšanas secība dažādiem datoriem atšķiras, un to var mainīt, izmantojot utilītu Computer Setup (F10).

Ja izmantojāt Windows 9x DOS versiju, tiek parādīts ekrāns ar Windows logotipu. Ja nevēlaties, lai šis ekrāns tiktu rādīts, USB zibatmiņas datu nesēja saknes direktorijam pievienojiet nulles lieluma failu LOGO.SYS.

Atgriezieties sadaļā Kopēšana vairākos datoros 18. lpp.

Neatbalstītā USB zibatmiņas datu nesēja ierīce

Lai izveidotu sāknēšanas USB zibatmiņas datu nesēju, jābūt:

- USB zibatmiņas iekārtai
- sāknējamai DOS disketei ar FDISK vai SYS programmām (ja programma SYS nav pieejama, var lietot programmu FORMAT, taču tādā gadījumā tiks zaudēti visi USB zibatmiņas datu nesēja faili)
- datoram, kuru var sāknēt no USB zibatmiņas iekārtas

△ **UZMANĪBU!** Dažus vecākus datorus var neizdoties sāknēt no USB zibatmiņas iekārtas. Ja utilītas Computer Setup (F10) noklusētajā sāknēšanas secības sarakstā USB ierīce ir norādīta pirms cietā diska, datoru var sāknēt no USB zibatmiņas datu nesēja. Pretējā gadījumā jālieto sāknēšanas diskete.

1. Ja sistēmā ir PCI kartes, kurām pievienoti SCSI, ATA RAID vai SATA diskdziņi, izslēdziet datoru un atvienojiet strāvas vadu.

△ **UZMANĪBU!** Strāvas vadam JĀBŪT atvienotam.

2. Noņemiet datora pārsegu un izņemiet PCI kartes.

3. Ievietojiet USB zibatmiņas datu nesēju kādā no datora USB portiem un noņemiet visas pārējās USB atmiņas ierīces, izņemot USB diskešu diskdziņus. Uzlieciet datora pārsegu.

4. Pievienojiet strāvas vadu un ieslēdziet datoru.

5. Tūlīt pēc datora ieslēgšanas nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai ieietu datora uzstādīšanā. Nospiediet taustiņu Enter, lai apietu nosaukumlapu, ja tas ir nepieciešams.

PIEZĪME Ja taustiņš F10 netiek nospiests atbilstošajā brīdī, restartējiet datoru un vēlreiz nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai piekļūtu utilītai.

6. Dodieties uz **Advanced** (Papildu) > **PCI Devices** (PCI ierīces), lai atspējotu gan PATA, gan SATA kontrollerus. Atspējojot SATA kontrolleri, pierakstiet pieprasījumu IRQ, kuram šis kontrolleris ir piesaistīts. Vēlāk pieprasījums IRQ būs jāpiesaista no jauna. Izejiet no iestatījumiem, apstiprinot izmaiņas.

   SATA IRQ: _____

7. Ievietojiet diskešu diskdzinī sāknēšanas DOS disketi, kurā ietvertas programmas FDISK.COM un SYS.COM vai FORMAT.COM, pēc tam ieslēdziet datoru, lai veiktu sāknēšanu uz DOS disketi.

8. Palaidiet programmu FDISK un izdzēsiet esošos USB zibatmiņas datu nesēja nodalījumus. Izveidojiet jaunu nodalījumu un atzīmējiet to kā aktīvu. Izejiet no programmas FDISK, nospiežot taustiņu Esc.

9. Ja, izejot no programmas FDISK, sistēma netika automātiski restartēta, nospiediet taustiņu kombināciju Ctrl+Alt+Del, lai no jauna veiktu sāknēšanu uz DOS disketi.

10. Uzvednē **A:** ievadiet `FORMAT C: /S` un nospiediet taustiņu Enter. Programma Format veic USB zibatmiņas datu nesēja formatēšanu, pievieno sistēmas failus un prasa norādīt sējuma etiķeti.

11. Nospiediet taustiņu Enter, ja nevēlaties ievadīt etiķeti, vai ievadiet to, ja vēlaties.

12. Izslēdziet datoru un atvienojiet strāvas vadu. Atveriet datora pārsegu un no jauna uzstādiet noņemtās PCI kartes. Uzlieciet datora pārsegu.

13. Pievienojiet strāvas vadu, izņemiet disketi un ieslēdziet datoru.

14. Tūlīt pēc datora ieslēgšanas nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai ieietu datora uzstādīšanā. Nospiediet taustiņu Enter, lai apietu nosaukumlapu, ja tas ir nepieciešams.

15. Dodieties uz **Advanced** (Papildu) > **PCI Devices** (PCI ierīces) un no jauna iespējojiet PATA un SATA kontrollerus, kuri 6. darbībā tika atspējoti. Novietojiet SATA kontrolleri tā sākotnējā IRQ.

16. Saglabājiet izmaiņas un izejiet no programmas. Dators veiks sāknēšanu uz USB zibatmiņas datu nesēju kā uz C disku.

PIEZĪME Noklusētā sāknēšanas secība dažādiem datoriem atšķiras, un to var mainīt, izmantojot utilītu Computer Setup (F10). Skatiet instrukcijas *Utilītprogramma Computer Setup (F10)* .

Ja izmantojāt Windows 9x DOS versiju, tiek parādīts ekrāns ar Windows logotipu. Ja nevēlaties, lai šis ekrāns tiktu rādīts, USB zibatmiņas datu nesēja saknes direktorijam pievienojiet nulles lieluma failu LOGO.SYS.

Atgriezieties sadaļā Kopēšana vairākos datoros 18. lpp.

8 Divstāvokļu ieslēgšanas/izslēgšanas poga

Ja ir aktivizēts interfeiss Advanced Configuration and Power Interface (ACPI), strāvas pogu var lietot gan kā ieslēgšanas/izslēgšanas slēdzi, gan kā gaidstāves pogu. Gaidstāves režīmā dators pilnībā netiek izslēgts, bet tiek pārslēgts nodroses režīmā ar minimālu enerģijas patēriņu. Šādi var ātri samazināt enerģijas patēriņu, neizejot no lietojumprogrammām, un atgriezties iepriekšējā darba režīmā, nezaudējot datus.

Lai mainītu strāvas pogas konfigurāciju, veiciet šādas darbības:

1. Ar peles kreiso pogu noklikšķiniet uz pogas **Start Button** (Sākt), pēc tam atlasiet **Control Panel** (Vadības panelis) > **Power Options** (Enerģijas opcijas).
2. Logā **Power Options Properties** (Enerģijas opciju rekvizīti) izvēlieties cilni **Advanced** (Papildu).
3. Sadaļā **Power Button** (Strāvas poga) izvēlieties **Stand by** (Gaidstāve).

Kad strāvas pogu esat konfigurējis darbībai gaidstāves režīmā, nospiediet strāvas pogu, lai sistēma darbotos minimālas strāvas padeves režīmā (gaidstāvē). Nospiediet pogu vēlreiz, lai sistēma ātri atgrieztos pilnas jaudas režīmā. Lai sistēmai pilnībā atslēgtu strāvas padevi, nospiediet un turiet strāvas pogu četras sekundes.

△ **UZMANĪBU!** Nelietojiet strāvas pogu, lai izslēgtu datoru, ja sistēma reaģē; strāvas izslēgšana, neizmantojot operētājsistēmu, var bojāt cieto disku vai izraisīt datu zudumu.

9 HP vietnes atbalsts

HP inženieri rūpīgi pārbauda un atkļūdo HP un trešo pušu piegādātāju izstrādāto programmatūru, kā arī izstrādā operētājsistēmas atbalsta programmatūru, lai nodrošinātu HP datoru veiktspēju, saderību un uzticamību.

Pārejot uz jaunu vai mainītu operētājsistēmu, ir svarīgi lietot attiecīgajai operētājsistēmai izstrādātu atbalsta programmatūru. Ja plānojat palaist Microsoft Windows versiju, kas atšķiras no datorā iekļautās versijas, jāinstalē atbilstoši ierīču draiveri un utilītas, lai nodrošinātu visu līdzekļu atbalstu un pareizu darbību.

HP ir atvieglojusi jaunākās atbalsta programmatūras atrašanu, piekļuvi tai, kā arī tās novērtēšanu un instalēšanu. Programmatūru var lejupielādēt no http://www.hp.com/support.

Šajā Web vietā iekļauti jaunākie ierīču draiveri, utilītas un pārrakstāmās ROM attēli, kas nepieciešami, lai HP datoros palaistu jaunāko operētājsistēmu Microsoft Windows.

10 Nozares standarti

HP pārvaldības risinājumi ir saskaņoti ar citām sistēmu pārvaldības lietojumprogrammām un atbilst šādiem nozares standartiem:

- Web-Based Enterprise Management (WBEM)
- Windows Management Interface (WMI)
- Tehnoloģija Wake on LAN
- ACPI
- SMBIOS
- Pre-boot Execution (PXE) atbalsts

11 Datu izsekošana un drošība

Datorā iekļautais datu izsekošanas līdzeklis nodrošina galvenos izsekošanas datus, ko var pārvaldīt, izmantojot programmu HP Systems Insight Manager, HP Client Manager, HP Configuration Management un Asset Management risinājumus, kā arī citas sistēmas pārvaldības lietojumprogrammas. Vienlaidu automātiskā datu izsekošanas līdzekļa un šo produktu integrācija ļauj izvēlēties pārvaldības rīku, kas vislabāk atbilst konkrētajai videi, un racionāli ieguldīt līdzekļus esošajos rīkos.

HP piedāvā arī vairākus risinājumus, kas ļauj vadīt piekļuvi vērtīgiem komponentiem un informācijai. Ja ir instalēts līdzeklis HP Embedded Security for ProtectTools, tas novērš nesankcionētu piekļuvi datiem, kā arī pārbauda sistēmas integritāti un autentificē trešās puses lietotājus, kas mēģina piekļūt sistēmai. (Plašāku informāciju skatiet rokasgrāmatā *HP ProtectTools Security Manager Guide* (HP ProtectTools Security Manager rokasgrāmata), kas pieejama vietnē http://www.hp.com/products/security.) Drošības līdzekļi, piemēram, HP Embedded Security for ProtectTools, sensors Smart Cover Sensor un slēdzene Smart Cover Lock, kas pieejami atsevišķiem modeļiem, novērš nesankcionētu piekļuvi datora iekšējiem komponentiem. Atspējojot paralēlos, seriālos vai USB portus vai atspējojot noņemamo datu nesēju sāknēšanas iespēju, var aizsargāt vērtīgus datus. Memory Change un sensora Smart Cover Sensor brīdinājumus var automātiski pārsūtīt uz sistēmas pārvaldības lietojumprogrammām, lai tiktu nosūtīti proaktīvi paziņojumi par datora iekšējo komponentu mainīšanu.

PIEZĪME Līdzekļi HP Embedded Security for ProtectTools, sensors Smart Cover Sensor un slēdzene Smart Cover Lock ir iespējas, kas pieejamas atsevišķām sistēmām.

Lai pārvaldītu HP datora drošības iestatījumus, lietojiet šādas utilītas:

- Lokāli lietojiet utilītu Computer Setup. Plašāku informāciju un norādījumus par utilītas Computer Setup lietošanu skatiet iekļautajā *Utilītas Computer Setup (F10) rokasgrāmatā*. Dažos datoros ir arī HP BIOS Configuration for ProtectTools – ProtectTools Windows komponents, kas administratoriem no darbojošās operētājsistēmas ļauj konfigurēt BIOS drošības iestatījumus.
- Attālināti lietojiet programmatūru HP Client Manager no Symantec, HP Client Automation vai System Software Manager. Šī programmatūra nodrošina drošus drošības iestatījumus, saskaņotu ieviešanu un vadību.

Šajā tabulā un sadaļās sniegta informācija par datora drošības līdzekļu lokālo vadīšanu, izmantojot utilītu Computer Setup (F10).

Tabula 11-1 Drošības līdzekļu pārskats

Iespēja	Apraksts
Setup Password (Iestatījumu parole)	Ļauj iestatīt un aktivizēt iestatījumu (administratora) paroli. **PIEZĪME** Ja ir iestatīta iestatījumu parole, ir nepieciešams mainīt Computer Setup iespējas, pārrakstīt ROM un mainīt atsevišķus Windows standarta Plug and Play iestatījumus.

Tabula 11-1 Drošības līdzekļu pārskats (turpinājums)

Power-On Password	Ļauj iestatīt un aktivizēt ieslēgšanas paroli. Ieslēdzot tiek parādīta ieslēgšanas paroles uzvedne. Ja lietotājs neievada pareizo ieslēgšanas paroli, sāknēšana nenotiek. **PIEZĪME** Šī parole netiek prasīta, veicot silto sāknēšanu, piemēram, nospiežot taustiņu kombināciju Ctrl+Alt+Delete vai izvēloties opciju **Restart from Windows** (Restartēt no Windows), ja tas nav iespējots iestatījumā **Password Options** (Paroles opcijas) (sk. tālāk).
Password Options (Šī izvēle tiek rādīta tikai tad, ja ir iestatīta ieslēgšanas parole.)	Ļauj: • slēgt mantotos resursus (tiek rādīta tikai tad, ja ir iestatīta iestatīšanas parole); • iespējot/atspējot tīkla servera režīmu (tiek rādīta tad, ja ir iestatīta ieslēgšanas parole); • norādīt, vai siltajai sāknēšanai ir vajadzīga parole (Ctrl+Alt+Delete) (tiek rādīta tad, ja ir iestatīta ieslēgšanas parole); • iespējot/atspējot iestatījumu pārlūkošanas režīmu (tiek rādīts, ja ir iestatīta iestatījumu parole) (ļauj skatīt, bet ne mainīt F10 Setup Options, neievadot iestatījumu paroli). • Iespējojiet/atspējojiet obligāto paroli (tiek parādīta, ja iestatīta ieslēgšanas parole), kura, ja iestatīta, apiet bortierīces paroles tiltslēgu, lai atspējotu ieslēgšanas paroli. Papildinformāciju skatiet *Galddatora pārvaldības rokasgrāmatā*.
Smart Cover (Viedais vāks) (dažiem modeļiem)	Ļauj: • slēgt/atslēgt pārsega slēdzeni; • iestatīt Cover Removal Sensor (Pārsega noņemšanas sensors) opciju Disable (Atspējot), Notify User (Paziņot lietotājam) vai Setup Password (Iestatījuma parole). **PIEZĪME** *Notify User* brīdina lietotāju, ka sensors ir noteicis pārsega noņemšanu. Iespēja *Setup Password* pieprasa ievadīt iestatījumu paroli, lai sāknētu datoru, ja sensors ir noteicis pārsega noņemšanu. Šis līdzeklis tiek atbalstīts tikai atsevišķiem modeļiem.
Device Security	Ļauj iestatīt opciju Device Available/Device Hidden (Ierīce pieejama/Ierīce paslēpta): • seriālie porti, • paralēlais ports, • aizmugurējie USB porti • priekšējais USB ports, • iekšējie USB porti • sistēmas audioierīces, • tīkla kontrolleri (dažiem modeļiem), • Mantota diskete • iegultā drošības ierīce (dažiem modeļiem). • SATA0 • SATA1 (dažiem modeļiem) • SATA2 (dažiem modeļiem) • SATA3 (dažiem modeļiem) • eSATA (dažiem modeļiem)

Tabula 11-1 Drošības līdzekļu pārskats (turpinājums)

Tīkla pakalpojumu sāknēšana	Iespējo/atspējo datora sāknēšanu no tīkla serverī instalētas operētājsistēmas. (Šis līdzeklis pieejams tikai NIC modeļiem; tīkla kontrollerim jābūt PCI paplašinājuma kartei vai jābūt iegultam sistēmas platē.)
System IDs	Ļauj iestatīt: • Līdzekļu tags (18 baitu identifikators), šim datoram piešķirtais uzņēmuma īpašuma identifikācijas numurs. • Īpašuma tagu (80 baitu identifikators), kas tiek parādīts POST darbības laikā. • Šasijas sērijas numuru un universālā unikālā identifikatora (UUID— Universal Unique Identifier) numuru. UUID var jaunināt tikai tad, ja pašreizējais šasijas sērijas numurs nav derīgs. (Parasti šie ID numuri tiek iestatīti rūpnīcā un lietoti, lai identificētu sistēmu.) • Tastatūras lokalizācijas iestatījumi (piemēram, angļu vai vācu), lai ievadītu sistēmas ID.
DriveLock Security (DriveLock drošības sistēma)	Ļauj piešķirt vai mainīt galveno vai lietotāja paroli cietajiem diskiem. Ja šis līdzeklis ir aktivizēts, POST darbības laikā lietotājam tiek piedāvāts ievadīt kādu no DriveLock parolēm. Ja nevienu paroli nevar veiksmīgi ievadīt, cietajam diskam nevarēs piekļūt līdz brīdim, kad kāda no parolēm tiks sekmīgi ievadīta nākošās aukstās sāknēšanas laikā. **PIEZĪME** Šī iespēja tiek rādīta tikai tad, ja sistēmai ir pieslēgts vismaz viens diskdzinis, kas atbalsta līdzekli DriveLock.
System Security (Sistēmas drošība) (dažiem modeļiem: šīs opcijas ir atkarīgas no aparatūras uzstādījumiem)	Data Execution Prevention (Datu izpildes novēršana) (dažiem modeļiem) (iespējot/atspējot). Palīdz novērst operētājsistēmas drošības uzlaušanu. Virtualization Technology (Virtualizācijas tehnoloģija) (dažiem modeļiem) (iespējot/atspējot) kontrolē procesora virtualizācijas līdzekļus. Lai mainītu šo iestatījumu, dators jāizslēdz un pēc tam jāieslēdz. Virtualization Technology Directed I/O (Virtualizācijas tehnoloģijas vadīta ievadizvade) (dažiem modeļiem) (iespējot/atspējot) kontrolē virtualizācijas DMA, pārkartējot mikroshēmas līdzekļus. Lai mainītu šo iestatījumu, dators jāizslēdz un pēc tam jāieslēdz. Trusted Execution Technology (Uzticamas izpildes tehnoloģija) (dažiem modeļiem) (iespējot/atspējot) kontrolē pamatā esošā procesora un mikroshēmas līdzekļus, kas nepieciešami virtuālās ierīces atbalstam. Lai mainītu šo iestatījumu, dators jāizslēdz un pēc tam jāieslēdz. Lai iespējotu šo līdzekli, jāiespējo šādi līdzekļi: • Embedded Security Device Support (Iegultas drošības ierīces atbalsts) • Virtualization Technology (Virtualizācijas tehnoloģija) • Virtualization Technology Directed I/O (Virtulizācijas tehnoloģijas vadīta ievadizvade) Embedded Security Device Support (Iegultas drošības ierīces atbalsts) (dažiem modeļiem) (iespējot/atspējot) ļauj aktivizēt/deaktivizēt iegultu drošības ierīci. Lai mainītu šo iestatījumu, dators jāizslēdz un pēc tam jāieslēdz. **PIEZĪME** Lai konfigurētu iegultu drošības ierīci, jāiestata iestatījumu parole. • Reset to Factory Settings (Atjaunot rūpnīcas iestatījumus) (dažiem modeļiem) (neatjaunot/atjaunot). Rūpnīcas noklusējumu atjaunošana dzēš visas drošības atslēgas. Lai mainītu šo iestatījumu, dators jāizslēdz un pēc tam jāieslēdz. **UZMANĪBU!** Iegulta drošības ierīce ir daudzu drošības shēmu kritisks komponents. Dzēšot drošības atslēgas, tiek liegta piekļuve datiem, ko aizsargā iegulta drošības ierīce. Izvēloties opciju Reset to Factory Settings (Atjaunot rūpnīcas iestatījumus), var zaudēt svarīgus datus. • Power-on authentication support (Ieslēgšanas autentificēšanas atbalsts) (dažiem modeļiem) (iespējot/atspējot) kontrolē ieslēgšanas paroles autentificēšanas shēmu, kas izmanto iegultu drošības ierīci. Lai mainītu šo iestatījumu, dators jāizslēdz un pēc tam jāieslēdz. • Reset authentication credentials (Atjaunot autentificēšanas pilnvaru) (dažiem modeļiem) (Neatjaunot/atjaunot). Atlasot opciju Reset (Atjaunot), tiek atspējots ieslēgšanas

Tabula 11-1 Drošības līdzekļu pārskats (turpinājums)

	autentificēšanas atbalsts un iegultā drošības ierīcē notīrīta informācija par autentificēšanu. Lai mainītu šo iestatījumu, dators jāizslēdz un pēc tam jāieslēdz. OS management of Embedded Security Device (Operētājsistēmas iegultās drošības ierīces pārvaldība) (dažiem modeļiem) (iespējot/atspējot)- šī opcija ļauj lietotājiem ierobežot operētājsistēmas kontroli pār iegultu drošības ierīci. Lai mainītu šo iestatījumu, dators jāizslēdz un pēc tam jāieslēdz. Šī opcija nodrošina, ka lietotājs var ierobežot operētājsistēmas kontroli pār iegultu drošības ierīci. • Reset of Embedded Security Device through OS (Iegultas drošības ierīces atiestatīšana, izmantojot operētājsistēmu) (dažiem modeļiem) (iespējot/atspējot) nodrošina, ka lietotājs var ierobežot operētājsistēmas iespēju pieprasīt opcijas Reset to Facory Settings of the Embedded Security Device (Atjaunot iegultas drošības ierīces rūpnīcas iestatījumus) izpildi. Lai mainītu šo iestatījumu, dators jāizslēdz un pēc tam jāieslēdz. **PIEZĪME** Lai iespējotu šo opciju, jāiestata iestatījumu parole. Smart Card BIOS Password Support (Viedkartes BIOS paroles atbalsts) (dažiem modeļiem) (iespējot/atspējot) ļauj lietotājam iespējot/atspējot viedkartes izmantošanu iestatījumu un ieslēgšanas paroļu vietā. Šim iestatījumam nepieciešama papildu ProtectTools inicializācija, pirms opcija sāk darboties. PAVP (dažiem modeļiem) (iespējots/min./maks.) iespējo aizsargāto audio video ceļu mikroshēmā. Tas var atļaut apskatīt aizsargātu augstas izšķirtspējas saturu, ko citādā veidā nevar atskaņot. Atlasot Maks., 96 megabaiti no sistēmas atmiņas tiks piešķirti tikai PAVP.
Setup Security Level (Iestatījumu drošības līmenis)	Nodrošina metodi, kas lietotājiem ļauj piešķirt ierobežotu piekļuvi iespējai mainīt norādītās iestatījumu opcijas bez nepieciešamības zināt iestatījumu paroli. Šis līdzeklis administratoram sniedz elastīgas iespējas aizsargāt svarīgu iestatījuma opciju izmaiņas, ļaujot lietotājam skatīt sistēmas iestatījumus un konfigurēt nebūtiskas opcijas. Administrators norāda piekļuves tiesības atsevišķām iestatījumu opcijām, izmantojot iestatījumu drošības līmeņa izvēlni. Pēc noklusējuma visām iestatījumu opcijām tiek piešķirta iestatījumu parole, norādot, ka lietotājam POST laikā ir jāievada pareizā iestatījumu parole, lai varētu mainīt kādu opciju. Administrators atsevišķiem elementiem var iestatīt vērtību None (Nav), norādot, ka lietotājs var veikt norādīto opciju izmaiņas, ja iestatījumiem tiek piekļūts, izmantojot nederīgu paroli. Ja iespējota ieslēgšana parole, izvēle None tiek aizstāta ar ieslēgšanas paroli. **PIEZĪME** Lai lietotājs piekļūtu iestatījumiem, nezinot iestatījumu paroli, ir jāiespējo iestatījumu pārlūkošanas režīms.

Paroles drošība

Ieslēgšanas parole novērš nesankcionētu datora lietošanu, pieprasot ievadīt paroli, lai piekļūtu lietojumprogrammām vai datiem, ikreiz, kad dators tiek ieslēgts vai restartēts. Iestatījumu parole īpaši novērš nesankcionētu piekļuvi utilītai Computer Setup, un to var lietot arī ieslēgšanas paroles vietā. Kad tiek parādīts uzaicinājums ievadīt ieslēgšanas paroli, tās vietā var ievadīt iestatījumu paroli, un piekļuve datoram tiek atļauta.

Var izveidot vispārēju tīkla paroli, kas sistēmas administratoram ļauj pieteikties visās tīkla sistēmās, lai veiktu apkopi, nezinot ieslēgšanas paroli, pat ja tā ir izveidota.

Iestatījumu paroles izveide, izmantojot utilītu Computer Setup

Ja sistēmā ir iegulta drošības ierīce, skatiet rokasgrāmatu *HP ProtectTools Security Manager Guide*, kas pieejama Web vietā http://www.hp.com. Ja iestatījumu parole ir izveidota, izmantojot utilītu

Computer Setup (F10), tad, lietojot šo utilītu, nevar veikt datora atkārtotu konfigurāciju, līdz tiek ievadīta parole.

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start** (Sākt) > **Shut Down** (Beidzēt) > **Restart** (Restartēt).

2. Tūlīt pēc datora ieslēgšanas nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai ieietu datora uzstādīšanā. Nospiediet taustiņu Enter, lai apietu nosaukumlapu, ja tas ir nepieciešams.

PIEZĪME Ja taustiņš F10 netiek nospiests atbilstošajā brīdī, restartējiet datoru un vēlreiz nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai piekļūtu utilītai.

3. Izvēlieties **Security** (Drošība), pēc tam izvēlieties **Setup Password** (Iestatījumu parole) un izpildiet ekrānā redzamos norādījumus.

4. Pirms iziešanas no programmas noklikšķiniet uz **File** (Fails) > **Save Changes and Exit** (Saglabāt izmaiņas un Iziet).

Ieslēgšanas paroles izveide, izmantojot utilītu Computer Setup

Ja ieslēgšanas parole ir izveidota, izmantojot utilītu Computer Setup, datoram nevar piekļūt, kad ir ieslēgta strāva, līdz tiek ievadīta parole. Ja ir iestatīta ieslēgšanas parole, utilītas Computer Setup izvēlnē **Security** (Drošība) ir pieejama iespēja **Password Options** (Paroles opcijas). Paroles opcijas ietver **Password Prompt on Warm Boot** (Jautāt paroli, veicot silto sāknēšanu). Ja ir aktivizēta iespēja **Password Prompt on Warm Boot**, parole ir jāievada ikreiz, kad dators tiek atsāknēts.

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start** (Sākt) > **Shut Down** (Beidzēt) > **Restart** (Restartēt).

2. Tūlīt pēc datora ieslēgšanas nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai ieietu datora uzstādīšanā. Nospiediet taustiņu Enter, lai apietu nosaukumlapu, ja tas ir nepieciešams.

PIEZĪME Ja taustiņš F10 netiek nospiests atbilstošajā brīdī, restartējiet datoru un vēlreiz nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai piekļūtu utilītai.

3. Izvēlieties **Security** (Drošība), pēc tam izvēlieties **Power-On Password** (Ieslēgšanas parole) un izpildiet ekrānā redzamos norādījumus.

4. Pirms iziešanas no programmas noklikšķiniet uz **File** (Fails) > **Save Changes and Exit** (Saglabāt izmaiņas un Iziet).

Ieslēgšanas paroles ievadīšana

Lai ievadītu ieslēgšanas paroli, veiciet šādas darbības:

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start** (Sākt) > **Shut Down** (Beidzēt) > **Restart the Computer** (Restartēt datoru).

2. Kad monitorā tiek parādīta atslēgas ikona, ievadiet pašreizējo paroli un nospiediet taustiņu Enter.

PIEZĪME Paroli ievadiet uzmanīgi; drošības apsvērumu dēļ ievadītās rakstzīmes ekrānā nav redzamas.

Ja parole ievadīta nepareizi, tiek parādīta salauztas atslēgas ikona. Mēģiniet vēlreiz. Pēc trīs neveiksmīgiem mēģinājumiem dators jāizslēdz un pēc tam no jauna jāieslēdz, lai turpinātu darbu.

Iestatījumu paroles ievadīšana

Ja sistēmā ir iegulta drošības ierīce, skatiet rokasgrāmatu *HP ProtectTools Security Manager Guide*, kas pieejama Web vietā http://www.hp.com.

Ja datoram ir izveidota iestatījumu parole, ikreiz, palaižot utilītu Computer Setup, tiek lūgts ievadīt šo paroli.

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start** (Sākt) > **Shut Down** (Beidzēt) > **Restart** (Restartēt).
2. Tūlīt pēc datora ieslēgšanas nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai ieietu datora uzstādīšanā. Nospiediet taustiņu Enter, lai apietu nosaukumlapu, ja tas ir nepieciešams.

PIEZĪME Ja taustiņš F10 netiek nospiests atbilstošajā brīdī, restartējiet datoru un vēlreiz nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai piekļūtu utilītai.

3. Kad monitorā tiek parādīta atslēgas ikona, ievadiet iestatījumu paroli un nospiediet taustiņu Enter.

PIEZĪME Paroli ievadiet uzmanīgi; drošības apsvērumu dēļ ievadītās rakstzīmes ekrānā nav redzamas.

Ja parole ievadīta nepareizi, tiek parādīta salauztas atslēgas ikona. Mēģiniet vēlreiz. Pēc trīs neveiksmīgiem mēģinājumiem dators jāizslēdz un pēc tam no jauna jāieslēdz, lai turpinātu darbu.

Ieslēgšanas vai iestatījumu paroles maiņa

Ja sistēmā ir iegulta drošības ierīce, skatiet rokasgrāmatu *HP ProtectTools Security Manager Guide*, kas pieejama Web vietā http://www.hp.com.

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start** (Sākt) > **Shut Down** (Beidzēt) > **Restart the Computer** (Restartēt datoru).
2. Lai mainītu ieslēgšanas paroli, pārejiet pie 3. darbības.

   Lai mainītu uzstādīšanas paroli, tūlīt pēc datora ieslēgšanas nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai ieietu datora uzstādīšanā. Nospiediet taustiņu Enter, lai apietu nosaukumlapu, ja tas ir nepieciešams.

PIEZĪME Ja taustiņš F10 netiek nospiests atbilstošajā brīdī, restartējiet datoru un vēlreiz nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai piekļūtu utilītai.

3. Kad tiek parādīta atslēgas ikona, ievadiet pašreizējo paroli, slīpsvītru (/) vai citu norobežotāju, jauno paroli, vēl vienu slīpsvītru (/) vai citu norobežotāju un vēlreiz — jauno paroli šādi: `pašreizējā parole/jaunā parole/jaunā parole`

PIEZĪME Paroli ievadiet uzmanīgi; drošības apsvērumu dēļ ievadītās rakstzīmes ekrānā nav redzamas.

4. Nospiediet taustiņu Enter.

Jaunā parole stājas spēkā, kad nākamo reizi ieslēgsit datoru.

PIEZĪME Plašāku informāciju par alternatīviem norobežotājiem skatiet Dažādām valodām paredzēto tastatūru norobežotāji 31. lpp. Ieslēgšanas paroli un iestatījumu paroli var mainīt arī, izmantojot utilītas Computer Setup iespēju Security (Drošība).

Ieslēgšanas vai iestatījumu paroles dzēšana

Ja sistēmā ir iegulta drošības ierīce, skatiet rokasgrāmatu *HP ProtectTools Security Manager Guide*, kas pieejama Web vietā http://www.hp.com.

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start** (Sākt) > **Shut Down** (Beidzēt) > **Restart the Computer** (Restartēt datoru).
2. Lai dzēstu ieslēgšanas paroli, pārejiet pie 3. darbības.

   Lai izdzēstu uzstādīšanas paroli, tūlīt pēc datora ieslēgšanas nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai ieietu datora uzstādīšanā. Nospiediet taustiņu Enter, lai apietu nosaukumlapu, ja tas ir nepieciešams.

PIEZĪME Ja taustiņš F10 netiek nospiests atbilstošajā brīdī, restartējiet datoru un vēlreiz nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai piekļūtu utilītai.

3. Kad tiek parādīta atslēgas ikona, ievadiet pašreizējo paroli, pēc tam slīpsvītru vai citu norobežotāju šādi: `pašreizējā parole/`
4. Nospiediet taustiņu Enter.

PIEZĪME Plašāku informāciju par alternatīviem norobežotājiem skatiet Dažādām valodām paredzēto tastatūru norobežotāji 31. lpp. Ieslēgšanas paroli un iestatījumu paroli var mainīt arī, izmantojot utilītas Computer Setup iespēju Security (Drošība).

Dažādām valodām paredzēto tastatūru norobežotāji

Katra tastatūra ir izstrādāta atbilstoši attiecīgās valsts prasībām. Sintakse un taustiņi, ko izmantojat, lai mainītu vai dzēstu paroli, ir atkarīgi no datora komplektācijā iekļautās tastatūras.

Dažādām valodām paredzēto tastatūru norobežotāji

/	Arābu	-	Grieķu	/	Krievu
=	Beļģu	.	Ebreju	-	Slovāku
-	BHMSS*	-	Ungāru	-	Spāņu
/	Brazīliešu	-	Itāliešu	/	Zviedru/somu
/	Ķīniešu	/	Japāņu	-	Šveiciešu
-	Čehu	/	Korejiešu	/	Taivāniešu
-	Dāņu	-	Latīņamerikāņu	/	Taizemiešu
!	Franču	-	Norvēģu	.	Turku
é	Kanādas franču	-	Poļu	/	ASV angļu
-	Vācu	-	Portugāļu		

* Bosnijai-Hercogovinai, Horvātijai, Melnkalnei, Serbijai un Slovēnijai

Paroļu notīrīšana

Ja esat aizmirsis paroli, datoram piekļūt nav iespējams. Instrukcijas par paroļu notīrīšanu skatiet *Problēmu novēršanas rokasgrāmatā*.

Ja sistēmā ir iegulta drošības ierīce, skatiet rokasgrāmatu *HP ProtectTools Security Manager Guide*, kas pieejama Web vietā http://www.hp.com.

DriveLock

DriveLock ir nozares standartiem atbilstošs drošības līdzeklis, kas novērš nesankcionētu piekļuvi datiem ATA cietajā diskā. DriveLock ir izstrādāts kā utilītas Computer Setup paplašinājums. Pieejams tikai tad, ja tiek atrasts cietais disks, kas atbalsta ATA drošības komandu. Līdzeklis DriveLock ir piemērots tiem HP klientiem, kuri vislielāko vērību pievērš datu drošībai. Šiem klientiem cietā diska izmaksas un tajā glabāto datu zudums nav būtisks salīdzinājumā ar kaitējumu, kas var rasties, nesankcionēti piekļūstot cietā diska saturam. Lai vienlaikus panāktu šāda līmeņa drošību un atrisinātu praktisku problēmu, ja aizmirsta parole, HP ir ieviesusi DriveLock divu paroļu drošības sistēmu. Vienu paroli iestata un lieto sistēmas administrators, bet otru parasti iestata un lieto galalietotājs. Ja abas paroles tiek pazaudētas, disku nav iespējams atbloķēt. Tāpēc DriveLock visdrošāk var lietot, ja cietajā diskā esošie dati tiek replicēti uzņēmuma informācijas sistēmā vai tiek regulāri veidotas to dublējumkopijas. Ja abas DriveLock paroles tiek pazaudētas, cietais disks vairs nav lietojams. Lietotāji, kuru vajadzības atšķiras no iepriekš aprakstīto klientu vajadzībām, šādu risku, iespējams, neuzņemas. Lietotājiem, kas atbilst šo klientu aprakstam, šāds risks ir pieņemams, ņemot vērā cietajā diskā glabāto datu saturu.

Izmantojot DriveLock

Ja atrasts vismaz viens cietais disks, kas atbalsta ATA drošības komandu, utilītas Computer Setup izvēlnē Security (Drošība) kļūst pieejama opcija DriveLock. Lietotājam tiek piedāvāta iespēja iestatīt galveno paroli vai aktivizēt līdzekli DriveLock. Lai aktivizētu līdzekli DriveLock, ir jāievada lietotāja parole. Tā kā DriveLock sākotnējo konfigurāciju parasti veic sistēmas administrators, vispirms ir jāiestata galvenā parole. HP sistēmas administratoriem iesaka iestatīt galveno paroli neatkarīgi no tā, vai tie plāno aktivizēt līdzekli DriveLock. Tādējādi nākotnē administrators var mainīt DriveLock iestatījumus, ja disks ir bloķēts. Kad galvenā parole ir iestatīta, sistēmas administrators var aktivizēt līdzekli DriveLock vai arī atstāt to deaktivizētu.

Ja cietais disks ir bloķēts, POST pieprasa paroli, lai atbloķētu ierīci. Ja iestatītā ieslēgšanas parole sakrīt ar ierīces lietotāja paroli, POST neprasa lietotājam paroli ievadīt no jauna. Pretējā gadījumā lietotājam tiek pieprasīts ievadīt DriveLock paroli. Veicot auksto sāknēšanu, var lietot gan galveno, gan lietotāja paroli. Siltās sāknēšanas laikā ievadiet to pašu paroli, kas diskdziņa atbloķēšanai lietota iepriekšējās aukstās sāknēšanas laikā. Lietotājs var divreiz mēģināt ievadīt pareizu paroli. Ja, veicot auksto sāknēšanu, šie mēģinājumi neizdodas, POST turpina darbību, taču disks nav pieejams. Veicot silto sāknēšanu vai Windows restartēšanu, ja nav sekmīgu mēģinājumu, POST tiek apturēta un lietotājam tiek likts ieslēgt/izslēgt strāvu.

DriveLock lietojumprogrammas

Vispraktiskāk drošības līdzekli DriveLock lietot uzņēmumā. Sistēmas administrators ir atbildīgs par cieto disku konfigurēšanu, kas ietver arī DriveLock galvenās paroles un pagaidu lietotāja paroles iestatīšanu. Ja lietotājs aizmirst lietotāja paroli vai aprīkojums tiek nodots citam darbiniekam, galveno paroli vienmēr var izmantot, lai no jauna iestatītu lietotāja paroli un atjaunotu piekļuvi cietajam diskam.

HP iesaka uzņēmumu sistēmas administratoriem, kas vēlas aktivizēt līdzekli DriveLock, izstrādāt uzņēmuma politiku galveno paroļu iestatīšanai un uzturēšanai. Šādi ir jārīkojas, lai nepieļautu situāciju, kad darbinieks pirms aiziešanas no uzņēmuma tīši vai netīši iestata abas DriveLock paroles. Tādā gadījumā cietais disks kļūst nederīgs un ir jānomaina. Ja galvenā parole nav iestatīta, var būt bloķēta sistēmas administratora piekļuve cietajam diskam un nevar veikt regulāras neautorizētas programmatūras pārbaudes, kā arī nevar īstenot citu līdzekļu vadības funkcijas un atbalstu.

Lietotājiem, kuriem nav tik stingru drošības prasību, HP neiesaka aktivizēt līdzekli DriveLock. Tie ir personālo datoru lietotāji vai lietotāji, kas cietajā diskā nemēdz glabāt slepenus datus. Šiem lietotājiem cietā diska zaudējums, kas iespējams, ja aizmirstas abas paroles, ir daudz būtiskāks nekā DriveLock aizsargāto datu vērtība. Piekļuvi utilītai Computer Setup un līdzeklim DriveLock var ierobežot, izmantojot iestatījumu paroli. Nosakot iestatījumu paroli, kas netiek atklāta galalietotājiem, sistēmas administrators var nepieļaut līdzekļa DriveLock aktivizēšanu.

Sensors Smart Cover Sensor

Cover Removal Sensor (Pārsega noņemšanas sensors), kas pieejams dažiem modeļiem, ir aparatūras un programmatūras tehnoloģijas kombinācija, kas var brīdināt, ja ir noņemts datora pārsegs vai sānu panelis. Šajā tabulā ir aprakstīti trīs aizsardzības līmeņi.

Tabula 11-2 Smart Cover Sensor aizsardzības līmeņi

Līmenis	Iestatījums	Apraksts
0. līmenis	Deaktivizēts	Sensors Smart Cover Sensor ir deaktivizēts (noklusējuma iestatījums).
1. līmenis	Paziņot lietotājam	Kad dators tiek restartēts, ekrānā tiek parādīts paziņojums par to, ka ir noņemts datora pārsegs vai sānu panelis.
2. līmenis	Setup Password (Iestatījumu parole)	Kad dators tiek restartēts, ekrānā tiek parādīts paziņojums par to, ka ir noņemts datora pārsegs vai sānu panelis. Lai turpinātu, ir jāievada iestatījumu parole.

PIEZĪME Šos iestatījumus var mainīt, izmantojot utilītu Computer Setup. Papildinformāciju par utilītu Computer Setup skatiet *utilītas Computer Setup (F10) rokasgrāmatā*.

Smart Cover Sensor drošības līmeņa iestatīšana

Lai iestatītu Smart Cover Sensor aizsardzības līmeni, izpildiet šādas darbības:

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start** (Sākt) > **Shut Down** (Beidzēt) > **Restart** (Restartēt).
2. Tūlīt pēc datora ieslēgšanas nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai ieietu datora uzstādīšanā. Nospiediet taustiņu Enter, lai apietu nosaukumlapu, ja tas ir nepieciešams.

PIEZĪME Ja taustiņš F10 netiek nospiests atbilstošajā brīdī, restartējiet datoru un vēlreiz nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai piekļūtu utilītai.

3. Atlasiet **Security** (Drošība) > **Smart Cover** (Viedais pārsegs) > **Cover Removal Sensor** (Pārsega noņemšanas sensors) un atlasiet nepieciešamo drošības līmeni.
4. Pirms iziešanas no programmas noklikšķiniet uz **File** (Fails) > **Save Changes and Exit** (Saglabāt izmaiņas un Iziet).

Smart Cover Lock

Slēdzene Smart Cover Lock ir ar programmatūru vadāma pārsega slēdzene, kas pieejama atsevišķiem HP datoriem. Šī slēdzene novērš nesankcionētu piekļuvi iekšējiem komponentiem. Iegādājoties datoru, slēdzene Smart Cover Lock ir atslēgtā stāvoklī.

△ **UZMANĪBU!** Lai gūtu maksimālu pārsega bloķēšanas drošību, norādiet uzstādīšanas paroli. Uzstādīšanas parole novērš nesankcionētu piekļuvi datora uzstādīšanas utilītai.

PIEZĪME Slēdzene Smart Cover Lock ir iespēja, kas pieejama atsevišķām sistēmām.

Slēdzenes Smart Cover Lock aizslēgšana

Lai aktivizētu un aizslēgtu slēdzeni Smart Cover Lock, veiciet šādas darbības:

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start** (Sākt) > **Shut Down** (Beidzēt) > **Restart** (Restartēt).
2. Tūlīt pēc datora ieslēgšanas nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai ieietu datora uzstādīšanā. Nospiediet taustiņu Enter, lai apietu nosaukumlapu, ja tas ir nepieciešams.

PIEZĪME Ja taustiņš F10 netiek nospiests atbilstošajā brīdī, restartējiet datoru un vēlreiz nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai piekļūtu utilītai.

3. Atlasiet **Security** (Drošība) > **Smart Cover** (Viedais pārsegs) > **Cover Lock** (Pārsega slēdzene) > **Lock option** (Slēgšanas opcija).
4. Pirms iziešanas no programmas noklikšķiniet uz **File** (Fails) > **Save Changes and Exit** (Saglabāt izmaiņas un Iziet).

Slēdzenes Smart Cover Lock atslēgšana

1. Ieslēdziet vai restartējiet datoru. Ja lietojat operētājsistēmu Windows, noklikšķiniet uz **Start** (Sākt) > **Shut Down** (Beidzēt) > **Restart** (Restartēt).
2. Tūlīt pēc datora ieslēgšanas nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai ieietu datora uzstādīšanā. Nospiediet taustiņu Enter, lai apietu nosaukumlapu, ja tas ir nepieciešams.

PIEZĪME Ja taustiņš F10 netiek nospiests pareizajā brīdī, restartējiet datoru un vēlreiz nospiediet taustiņu F10, pirms dators sāknē operētājsistēmu, lai piekļūtu utilītai.

3. Atlasiet **Security** (Drošība) > **Smart Cover** (Viedais pārsegs) > **Cover Lock** (Slēdzenes pārsegs) **Unlock** (Atslēgt).
4. Pirms iziešanas no programmas noklikšķiniet uz **File** (Fails) > **Save Changes and Exit** (Saglabāt izmaiņas un Iziet).

Atslēgas Smart Cover FailSafe Key izmantošana

Ja ir aktivizēta slēdzene Smart Cover Lock, taču nevar ievadīt paroli, lai slēdzeni deaktivizētu, datora pārsegu var atvērt, izmantojot atslēgu Smart Cover FailSafe Key. Atslēga ir nepieciešama šādos gadījumos:

- Strāvas pārtraukums
- Startēšanas kļūme
- Datora komponenta (piemēram, procesora vai barošanas bloka) kļūme
- Aizmirsta parole

△ **UZMANĪBU!** Atslēga Smart Cover FailSafe Key ir specializēts rīks, kas pieejams no HP. Sagatavojieties; pasūtiet šo atslēgu no pilnvarota izplatītāja vai pakalpojumu sniedzēja, pirms jums tā ir vajadzīga.

Lai iegādātos atslēgu FailSafe Key, veiciet kādu no šīm darbībām:

- Sazinieties ar pilnvarotu HP izplatītāju vai pakalpojumu sniedzēju.
- Zvaniet uz garantijā norādīto atbilstošo numuru.

Plašāku informāciju par atslēgas Smart Cover FailSafe Key lietošanu skatiet iekļautajā *Aparatūras rokasgrāmatā*.

Kabeļa slēdzenes nodrošinājums

Datora aizmugures panelim (dažiem modeļiem) var uzstādīt kabeļa slēdzeni, lai dators fiziski tiktu nostiprināts pie darba virsmas.

Ilustrētas instrukcijas, lūdzu, skatiet *Aparatūras rokasgrāmatā*.

Pirkstu nospiedumu identificēšanas tehnoloģija

Lai nebūtu jāievada lietotāju paroles, HP tehnoloģija Fingerprint Identification paaugstina tīkla drošību, vienkāršo pieteikšanās procesu un samazina ar kopējo tīklu pārvaldību saistītās izmaksas. Par pašreizējo cenu šo tehnoloģiju var atļauties iegādāties ne tikai progresīvo tehnoloģiju un augstas drošības organizācijas.

PIEZĪME Pirkstu nospiedumu identificēšanas tehnoloģijas atbalsts ir atkarīgs no datora modeļa.

Kļūmes paziņojums un atkopšana

Līdzekļi Fault Notification un Recovery apvieno jaunas aparatūru un programmatūras tehnoloģijas, kas novērš svarīgu datu zaudēšanu un samazina neplānotas dīkstāves risku.

Ja dators ir pieslēgts tīklam, ko pārvalda programmatūra HP Client Manager, dators nosūta kļūdas paziņojumu tīkla pārvaldības lietojumprogrammai. Izmantojot programmatūru HP Client Manager (HP klientu pārvaldnieks), var attāli plānot diagnostiku, lai to automātiski palaistu uz visiem pārvaldītajiem datoriem un izveidotu kopsavilkuma atskaiti par neapmierinošajiem pārbaužu rezultātiem.

Disku aizsardzības sistēma

Drive Protection System (DPS) ir cietajā diskā iebūvēts diagnostikas rīks, kas uzstādīts atsevišķiem HP datoriem. DPS ir paredzēts to problēmu noteikšanai, kas varētu izraisīt cietā diska aizstāšanu bez garantijas.

Montējot HP datorus, katrs uzstādītais cietais disks tiek pārbaudīts, izmantojot DPS, un šajā diskā tiek izveidots pamatinformācijas pastāvīgais ieraksts. Ikreiz, kad tiek palaista DPS, testa rezultāti tiek rakstīti cietajā diskā. Pakalpojumu sniedzējs var izmantot šo informāciju, lai diagnosticētu apstākļus, kuros tika palaista DBS programmatūra. Instrukcijas par DPS izmantošanu skatiet *Problēmu novēršanas rokasgrāmatā*.

Izlīdzinošs barošanas bloks

Iebūvēts izlīdzinošais barošanas bloks sniedz drošību, ja notiek neparedzēta strāvas pārslodze. Šis barošanas bloks var izturēt ne vairāk kā 2000 voltu strāvas pārslodzi, neradot sistēmas dīkstāvi vai datu zudumu.

Termiskais sensors

Termiskais sensors ir aparatūras un programmatūras līdzeklis, kas izseko datora iekšējo temperatūru. Šis līdzeklis parāda brīdinājuma ziņojumu, kad tiek pārsniegts parastais diapazons, kas dod laiku darbībai, pirms tiek bojāti iekšējie komponenti vai rodas datu zudumi.

△ **UZMANĪBU!** Augsta temperatūra var izraisīt sistēmas bojājumus vai datu zudumus.

Alfabētiskais rādītājs