SMLOUVA
o dodávce úložných kapacit pro nepřepisovatelné zálohy (offline) včetně poskytování podpory

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), mezi:

Českou národní bankou

Na Příkopě 28
115 03 Praha 1
zastoupenou: Ing. Milanem Zirnsákem, ředitelem sekce informatiky
a
Ing. Zdeňkem Viriusem, ředitelem sekce správní
IČO: 48136450
DIČ: CZ48136450

(dále jen „objednatel“ nebo také „ČNB“)

a

KLARI s.r.o.

zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl C, vložka 171726
sídlo: Antala Staška 2027/77, 140 00 Praha 4

IČO: 24756679
DIČ: CZ24756679
zastoupená: Ing. Lumírem Bolkem, jednatelem
č. účtu: 5484305339/0800 (plátce DPH uvede svůj účet, který je zveřejněn podle § 98 zákona o DPH)

(dále jen „zhotovitel“, popř. „dodavatel“)

Článek I.
Předmět plnění

1. Zhotovitel se zavazuje dodat, nainstalovat, zprovoznit a implementovat technické a programové prostředky pro ukládání záloh vytvořených SW Microfocus DataProtector tak, aby tyto kopie nebylo možné smazat nebo modifikovat. Technické a programové prostředky musí splňovat funkční požadavky uvedené v příloze č. 4 a systém zálohování s implementovanými technickými a programovými prostředky musí trvale, zejména však během zkušebního provozu, vykazovat požadované hodnoty podle přílohy č. 10. Předmět plnění musí být realizován v souladu s návrhem technického řešení obsaženým v nabídce zhotovitele (příloha č. 5). Technické a programové prostředky, které zhotovitel dodá v rámci implementace systému zálohování, jsou uvedeny v příloze č. 1 této smlouvy.

2. Součástí plnění dle odstavce 1 je dále:
   a) vypracování realizačního projektu;
   b) dodávka licencí Microfocus DataProtector;
   c) provedení zaškolení zaměstnanců objednatele;
   d) dodání uživatelské / administrátorské dokumentace výrobce technických prostředků a dokumentace programových prostředků;
   e) pomoc zaměstnancům objednatele při migraci v oblasti DataProtector a asistence pracovníků zhotovitele při zkušebním provozu;
   f) vypracování dokumentace v souladu s přílohou č. 11 k systému zálohování po implementaci technických a programových prostředků podle odst. 1 (dále jen „realizační dokumentace“) v elektronické podobě ve formátu MS Word 2010 a vyšším.
3. Zhotovitel se rovněž zavazuje poskytovat objednateli podporu pro dodané technické a programové prostředky, blíže specifikovanou v čl. VII této smlouvy.
4. **Dodané technické prostředky podle této smlouvy budou nové a nepoužité** (maximálně z továrny zahořelé z výroby nebo zapnuté pro ověření funkčnosti v rámci kompletace prostředků zhotovitelem před dodáním). Uvedené se týká i všech komponent (zejména všech typů disků, SFP modulů, zdrojů apod.).
5. Technické a programové prostředky podle odst. 1 musí být implementovány v souladu s realizačním projektem podle odst. 2 písm. a) tohoto článku. Zaškolení zahrnuje seznámení odborných zaměstnanců objednatele s běžnou obsluhou předmětných prostředků.
6. Zhotovitel bere na vědomí, že k technickým ani programovým prostředkům nebude zhotoviteli poskytován vzdálený přístup.
7. Objednatel se zavazuje za poskytnutá plnění uhradit ceny dle čl. IV této smlouvy.

Článek II.
Průběh díla

Plnění podle čl. I odst. 1 až 3 (dále též „dílo“) bude realizováno ve třech dílčích plněních takto:

a) **první dílčí plnění zahrnuje** vypracování realizačního projektu, který bude obsahovat veškeré informace nezbytné pro implementaci technických a programových prostředků do prostředí objednatele (viz příloha č. 3), postup migrace dat a harmonogram plnění dle čl. I odst. 1 a 2 této smlouvy; v závislosti na konkrétní použité technologii bude realizační projekt obsahovat zejména informace podle přílohy č. 9 této smlouvy;

b) **druhé dílčí plnění zahrnuje**

- dodávku technických a programových prostředků podle specifikace uvedené v příloze č. 1 včetně dokumentace podle čl. I odst. 2 písm. d);
- instalaci a zprovoznění technických a programových prostředků a jejich implementaci do prostředí objednatele (zapojení do SAN/LAN), konfiguraci dodaných prostředků, připojení k serverům objednatele (2 Windows servery pro zálohování) a konfiguraci DataProtector pro práci s dodanými prostředky;

- instalaci managementu dodaných technických a/nebo programových prostředků (konfigurace prostředků, hlášení závad, atd.), bude-li to nutné v závislosti na konkrétní použité technologii a konkrétních dodaných prostředcích;
- vypracování popisu postupů správy implementovaných technických a programových prostředků a jejich maximální automatizace (např. scripty) v různých případech havárií nebo při běžných činnostech (v závislosti na navrženém řešení), např.:
    - přesměrování drivů DataProtector při výpadku knihovny (offline kopie);
    - aktualizace informace o médiích v DataProtector v případě kopírování médií interně mezi knihovnami;
- zaškolení zaměstnanců objednatele podle čl. I odst. 2 písm. c) přímo na dodávaných technických a programových prostředcích v rozsahu dle návrhu zhotovitele, minimálně však 5 hodin;

c) **třetí dílčí plnění zahrnuje**:

- odstranění nalezených nedostatků nejpozději do 3 týdnů od ukončení penetračního testování, které objednatel provede na své náklady, a to za účelem ověření nesmazatelnosti a neměnnosti uložených dat;
- pomoc zaměstnancům objednatele při vytváření dalších kopií dat (offline) v oblasti DataProtector asistence pracovníků zhotovitele při zkušebním provozu podle čl. I odst. 2 písm. e);
- vypracování realizační dokumentace podle čl. I odst. 2 písm. f) o obsahu dle přílohy č. 11 této smlouvy.

Článek III.
Místo plnění, lhůty a předání a převzetí dílčích plnění

1. Smluvní strany vzájemně dohodly pro jednotlivá (dílčí) plnění následující lhůty:
    a) zhotovitel předá první dílčí plnění do 4 týdnů ode dne podpisu smlouvy;
    b) zhotovitel do 14 týdnů ode dne podpisu smlouvy vypracuje a předá objednateli popisy postupů správy a jejich maximální automatizace podle čl. II písm. b) čtvrté odrážky (část druhého dílčího plnění);
    c) zhotovitel předá druhé dílčí plnění nejpozději do 20 týdnů ode dne podpisu smlouvy;
    d) zhotovitel předá třetí dílčí plnění do 30 týdnů od podpisu smlouvy.
2. Lhůty podle odst. 1 je oprávněna (nikoliv povinna) kterákoliv z pověřených osob objednatele podle čl. VI odst. 5 na písemnou a odůvodněnou žádost zhotovitele přiměřeně okolnostem prodloužit, a to po zvážení všech objektivních okolností zhotovitelem v jeho žádosti uvedených anebo objednateli známých (včetně např. zdržení v dodavatelsko-odběratelském řetězci, ale ne z důvodů na straně zhotovitele, nebo okolností majících původ na straně objednatele), majících vliv na možnosti zhotovitele plnit v předmětných lhůtách. Zhotovitel je povinen na žádost objednatele kteroukoliv jím tvrzenou skutečnost (okolnost) doložit.
3. Místem plnění budou prostory výpočetního střediska v objektu objednatele na adrese Praha 1, Senovážná ul. 3.

4. O předání a převzetí jednotlivých dílčích plnění sepíše zhotovitel protokol, který podepíší pověřené osoby obou smluvních stran. Bude-li dílčí plnění k okamžiku předání a převzetí obsahovat závady nebo nedodělky, které nebrání jeho užívání, budou tyto v protokolu popsány společně se lhůtou k jejich odstranění, na které se strany dohodnou. Objednatel není povinen převzít dílčí plnění vykazující závady nebo nedodělky a nepřevezme dílčí plnění vykazující takové závady nebo nedodělky, které brání jeho užívání.

Článek IV.
Cena plnění a platební podmínky

1. Ceny plnění uvedené v odst. 2 až 4 byly stanoveny dohodou smluvních stran bez DPH a zahrnují veškeré náklady zhotovitele spojené s plněním podle této smlouvy včetně odměn za poskytnutí licencí a u cen podpory uvedených v odst. 5 a 6 včetně náhradních dílů, dopravného apod. Specifikace cen je v příloze č. 8 této smlouvy.
2. Cena prvního dílčího plnění podle čl. I odst. 2 písm. a), resp. čl. II písm. a), činí celkem 80 000 Kč (slovy: osmdesát tisíc korun českých).
3. Cena druhého dílčího plnění podle čl. I odst. 1, 2 písm. b) a d), resp. čl. II písm. b), činí celkem 5 597 832 Kč (slovy: pět miliónů pět set devadesát sedm tisíc osm set třicet dva) korun českých), z toho cena za zaškolení zaměstnanců objednatele činí 24 000 Kč (slovy: dvacet čtyři tisíc korun českých).
4. Cena třetího dílčího plnění podle čl. I odst. 2 písm. e) a f), resp. čl. II písm. b), činí celkem 54 000 Kč (slovy: padesát čtyři tisíc korun českých).
5. Paušální cena za podporu technických prostředků činí měsíčně 8 000 Kč (slovy: osm tisíc korun českých).
6. Paušální cena za podporu programových prostředků činí měsíčně 8 000 Kč (slovy: osm tisíc korun českých).
7. Výše paušální ceny za období kratší, než je sjednané období, se vypočte jako alikvotní část sjednané ceny.
8. K cenám bude připočtena DPH v sazbě platné v den uskutečnění příslušného zdanitelného plnění.
9. Cena podle odst. 2 bude hrazena na základě daňového dokladu vystaveného zhotovitelem nejdříve v den podpisu protokolu o předání a převzetí prvního dílčího plnění.
10. Cena podle odst. 3 bude hrazena na základě daňového dokladu vystaveného zhotovitelem nejdříve v den podpisu protokolu o předání a převzetí druhého dílčího plnění.
11. Cena podle odst. 4 bude hrazena na základě daňového dokladu vystaveného zhotovitelem nejdříve v den podpisu protokolu o předání a převzetí třetího dílčího plnění.
12. Paušální ceny podle odst. 5 a 6 budou hrazeny měsíčně na základě jednoho daňového dokladu, vystaveného nejdříve poslední den měsíce, ve kterém bylo příslušné plnění poskytováno.
13. Doklady k úhradě (faktury) zašle zhotovitel elektronicky jako přílohu e-mailové zprávy na adresu faktury@cnb.cz ve formátu ISDOC. Pokud není možné vytvořit doklad ve formátu ISDOC, je možné zasílat jej ve formátu PDF. V jedné e-mailové zprávě smí být pouze jeden doklad k úhradě. Mimo vlastní doklad k úhradě může být přílohou e-mailové zprávy jedna až sedm příloh k dokladu ve formátech PDF, DOC, DOCX, XLS, XLSX. Přijaty budou i doklady k úhradě v jiném formátu, který bude v souladu s evropským standardem

elektronické faktury. Nebude-li možné zaslat doklad k úhradě elektronicky, zašle jej zhotovitel v analogové formě na adresu:

Česká národní banka
sekce rozpočtu a účetnictví
odbor účetnictví
Na Příkopě 28
115 03 Praha 1

14. Doklad k úhradě bude obsahovat údaje podle § 435 občanského zákoníku a bankovní účet, na který má být placeno, a který je uveden v záhlaví této smlouvy nebo který byl později aktualizován zhotovitelem (dále jen „určený účet“). Daňový doklad bude nadto obsahovat náležitosti stanovené v zákoně o dani z přidané hodnoty. Nezbytnou náležitostí každého dokladu je také číslo této smlouvy (ve formátu ISDOC v poli ID ve skupině Contract References). Pokud doklad bude postrádat některou ze stanovených náležitostí nebo bude obsahovat chybné údaje, je objednatel oprávněn jej vrátit zhotoviteli, a to až do lhůty splatnosti. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného dokladu.
15. V případě, že bude v dokladu k úhradě uveden jiný než určený účet, je pověřený pracovník zhotovitele povinen na základě výzvy objednatele sdělit na e-mailovou adresu, ze které byla výzva odeslána, zda má být zaplaceno na bankovní účet uvedený v dokladu, nebo na určený účet. V tomto případě se doklad k úhradě nevrací s tím, že lhůta splatnosti začíná běžet až dnem doručení sdělení zhotovitele podle předchozí věty.
16. Splatnost dokladů činí 14 dnů ode dne jejich doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu zhotovitele.
17. Smluvní strany se ve smyslu občanského zákoníku dohodly, že objednatel je oprávněn započíst jakoukoli svou peněžitou pohledávku za zhotovitelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce zhotovitele za objednatelem, ať splatné či nesplatné.

Článek V.
Zkušební provoz, návrh optimalizace a připomínky k realizační dokumentaci

1. Zkušební provoz bude probíhat po dobu **10 týdnů** v rámci realizace třetího dílčího plnění. Zkušební provoz bude spočívat v plném provozu dodaných a implementovaných technických a programových prostředků v prostředí objednatele (viz příloha č. 3), a to s cílem zjistit, zda implementované technické a programové prostředky splňují požadavky podle přílohy č. 4 a vykazují požadované hodnoty podle přílohy č. 10 tabulky.
2. V rámci zkušebního provozu provede objednatel na své náklady penetrační testy za účelem zjistit, zda není možné uložená data smazat nebo jakkoliv modifikovat.
3. Zhotovitel se zavazuje na vyžádání poskytnout asistenci svých pracovníků při zkušebním provozu a pomoc zaměstnancům objednatele, a to jak telefonicky, tak v případě potřeby i v místě plnění dle této smlouvy. Zhotovitel bere na vědomí, že uvedené může zahrnovat i vysvětlování a ladění parametrů.
4. Zhotovitel v rámci zkušebního provozu, na základě údajů při něm získaných, vytvoří a předá objednateli návrh optimalizace systému zálohování s implementovanými technickými a programovými prostředky (viz též příloha č. 10).
5. Objednatel může zkušební provoz přerušit, pakliže se vyskytne v systému offline zálohování s implementovanými technickými a programovými prostředky závada bránící jeho pokračování. Objednatel může rozhodnout o opakování části nebo celého zkušebního

provozu, pakliže se vyskytne v systému zálohování s implementovanými technickými a programovými prostředky závada bránící dosažení cíle zkušebního provozu podle odst. 1. Lhůty podle čl. III odst. 1 tím nejsou dotčeny.

6. Objednatel je oprávněn k zhotovitelem zpřístupněné realizační dokumentaci vznést do 5 pracovních dnů od jejího zpřístupnění připomínky, na jejichž vypořádání poskytne zhotoviteli přiměřenou lhůtu, a to nejméně ve 2 opakováních. Nevypořádání připomínek objednatele se považuje za závadu realizační dokumentace. Lhůty podle čl. III odst. 1 tím nejsou dotčeny.

Článek VI.
Další povinnosti smluvních stran, pověřené osoby

1. Objednatel se zavazuje vytvořit zhotoviteli k instalaci potřebné podmínky, zejména:
   a) spolupracovat při vytváření realizačního projektu;
   b) zajistit provozní odstávky v přiměřeném rozsahu, a to nejvýše na 4 hodiny v souvislé době;
   c) poskytnout plán stávajícího propojení objektů, informace o používaném označení portů stávajících zařízení objednatele (DWDM, patch panely, servery), případně používaných konvencí pro tvorbu jejich označování, používané konvence pro označování portů v serverech a na paměťových zařízeních;
   d) umožnit prohlídku místa plnění s ohledem na fyzické umístění dodávaných prostředků;
   e) zajistit potřebné rekonfigurace všech technických a programových prostředků ČNB dotčených přechodem na dodávané prostředky, pokud tyto rekonfigurace nebudou v rozporu s jinými provozními požadavky ČNB;
   f) přidělit IP adresy pro dodávané prostředky pro potřeby managementu;
   g) přidělit nejvýše 4 porty na FC direktorech v každé lokalitě a/nebo 4 port ethernet 10 GBit/s;
   h) zajistit přístup odborných pracovníků zhotovitele na příslušná pracoviště objednatele;
   i) zajistit 1fázové napájení 230V se zakončením rozvodnou krabicí ve zdvojené podlaze nebo PDU ve stojanu (konektor C13/C19);
   j) zajistit prostor v 19“ stojanu dle parametrů uvedených v příloze č. 4;
   k) umožnit zhotoviteli vykládku a úschovu technických prostředků potřebných k plnění dle této smlouvy, jak jsou specifikovány v příloze č. 1, v prostorách objednatele určených k instalaci v termínu, o kterém byl zhotovitelem zpraven nejméně 3 pracovní dny předem;
   l) převzít prostředky podle písm. k) do úschovy a zajistit jejich bezpečné uskladnění do zahájení instalace. Objednatel není povinen převzít do úschovy prostředky, jejichž obal je poškozen nebo které samy jeví známky poškození bez ohledu na stav obalu. O předání prostředků do úschovy sepíše zhotovitel protokol, který podepíší pověřené osoby obou smluvních stran.

2. Zhotovitel je povinen vést deník o instalaci, tj. průběžně zaznamenávat provedené změny v celém průběhu instalace, zprovoznění a implementace technických a programových prostředků podle čl. I odst. 1 a zajišťovat zápisy z jednání, protokoly o předání funkčních celků a protokoly o zaškolení obsluhy. Informace z deníku o instalaci musí zhotovitel přenést do realizační dokumentace.

3. Při návrhu řešení a při své činnosti musí zhotovitel dodržet standardy objednatele a současně musí respektovat současnou infrastrukturu tak, aby nedošlo ke změnám, které by mohly ovlivnit funkčnost systémů objednatele. Jedná se zejména o dodržení specifikací uvedených v příloze č. 3 (popis současného stavu, standardy objednatele, kompatibilitu řešení se stávajícími technologiemi) a dodržení požadavků uvedených v přílohách č. 4 a 6 (požadované funkce a vlastnosti a zajištění dostatečné bezpečnosti).
4. Zhotovitel se zavazuje v plném rozsahu dodržovat bezpečnostní požadavky ČNB, které jsou uvedeny v příloze č. 7 této smlouvy.
5. Pověřenými osobami jsou:
   a) za objednatele:
   [redacted]
   b) za zhotovitele:
   [redacted]
6. Zhotovitel prohlašuje, že po dobu účinnosti této smlouvy bude mít sjednáno pojištění pro případ vzniku odpovědnosti za škodu způsobenou třetí osobě v souvislosti s plněním této smlouvy, a to s pojistným plněním ve výši nejméně 5 000 000 Kč (slovy: pět milionů korun českých) s tím, že jeho spoluúčast nepřevyšuje 5 %. Zhotovitel se zavazuje, že pojištění v uvedené výši a rozsahu zůstane účinné po celou dobu účinnosti této smlouvy a do 5 pracovních dnů od výzvy objednatele je zhotovitel povinen toto objednateli prokázat.

Článek VII.
Technická podpora

1. Zhotovitel se zavazuje poskytovat technickou podporu technických a programových prostředků ode dne podpisu protokolu o předání a převzetí druhého dílčího plnění.
2. Technická podpora zahrnuje:
   a) Odstraňování **kritických závad technických a programových prostředků**:
   Za kritickou závadu se považuje taková závada, kdy systém zálohování nemůže ukládat nebo číst data do/z libovolného z dodaných technických prostředků, a to i v důsledku závady libovolného z dodaných programových prostředků. Mezi kritické závady dále patří:
   - snížení výkonu pod 50 % požadovaného výkonu nebo požadované kapacity;
   - výpadek druhé z redundantních komponent (týká se zejména RAID 6 a výpadku 2 disků v rámci jedné paritní skupiny apod.).

   Odstranění kritických závad musí být dokončeno **do 24 hodin od nahlášení závady**. Pro nahlášení tohoto typu závady musí být dostupná hotline 24 hodin denně 7 dnů v týdnu. Údržbu SAN (Storage Area Network) zajišťuje objednatel, a proto řešení závad v této komponentě zhotovitel nezajišťuje;

   b) Odstraňování **nekritických závad technických prostředků:**
   Za nekritickou závadu se považuje taková závada dodaných technických prostředků, která neohrožuje vlastní provoz těchto prostředků, zejména:

- výpadek první z redundantních komponent;
- závady na managementu.

Odstranění nekritické závady musí být ukončeno **do 5 pracovních dnů od nahlášení**, nebude-li pověřenými osobami písemně dohodnuto jinak. Pro uskutečnění servisního zásahu techniků zhotovitele platí režim 5x9, tj. technici zhotovitele budou k dispozici v pracovní dny v době od 8:00 do 17:00 hod. Závada ohlášená po 17:00 hod. se považuje za nahlášenou v 8:00 hod. následující pracovní den.

c) Při vzniku **nekritické závady programových prostředků** bude zahájeno řešení závady nejpozději do 2 hodin po jejím ohlášení zhotoviteli. Na jejím odstranění musí zhotovitel pracovat bez neodůvodněného přerušení. Pro uskutečnění servisního zásahu techniků zhotovitele platí režim 5x9, tj. technici zhotovitele budou k dispozici v pracovní dny v době od 8:00 do 17:00 hod. Závada ohlášená po 17:00 hod. se považuje za nahlášenou v 8:00 hod. následující pracovní den.

3. Podpora technických prostředků nesmí být v jakékoliv formě (tj. ani ve formě záruční či pozáruční podpory výrobcem technického prostředku) jakkoliv limitována ve smyslu počtu provozních hodin za den/měsíc/rok nebo jiné časové údobí, počtu zápisových cyklů apod. Toto se netýká případného poškození způsobeného neodborným zásahem objednatele.
4. Zhotovitel v rámci podpory zajistí náhradní díly, nové a opravné verze mikrokódu/firmware dodaných technických prostředků a nové a opravné verze dodaných programových prostředků včetně jejich implementace/instalace. Součástí podpory je také:
   - informování objednatele o nových nebo opravných verzích;
   - konzultace k plánovaným změnám.
5. Zhotovitel je srozuměn s tím, že veškerá komunikace při implementaci, hlášení a řešení závad bude mezi objednatelem a technickými pracovníky zhotovitele probíhat v českém jazyce.
6. Služby poskytované zhotovitelem musí vyhovovat technickým specifikacím a požadavkům výrobce příslušného technického nebo programového prostředku. Požaduje-li nebo doporučuje-li výrobce technického nebo programového prostředku provádění podpory (instalace, opravy, úpravy aj.) pouze osobou s příslušnou výrobcem předepsanou kvalifikací, je zhotovitel povinen poskytovat podporu pro dodané technické a programové prostředky pouze pracovníky s takovou kvalifikací.
7. Požadavky na odstranění závad a na ostatní služby (odst. 4) podle této smlouvy budou nahlašovány na kontakt a způsobem uvedeným v příloze č. 2. Kritické závady objednatel současně vždy oznámí telefonicky **na číslo +420 720 030 613.** Přijetí požadavku na odstranění kritické závady je zhotovitel povinen potvrdit na kontakt uvedený v příloze č. 2 nejpozději do 2 hodin od nahlášení požadavku. Přijetí požadavku na odstranění nekritických závad technických i programových prostředků je zhotovitel povinen potvrdit do 2 hodin od nahlášení požadavku. O kategorizaci závady rozhoduje objednatel.
8. O každém provedeném servisním zásahu vede zhotovitel záznamy.
9. Zhotovitel se zavazuje převzít od objednatele vyměněné vadné díly a zajistit jejich likvidaci dle platných právních předpisů.
10. **Zhotovitel souhlasí s tím, že při výměně vadného disku nebo jiné komponenty umožňující trvalý záznam dat (např. magnetická páska) budou na vadném disku**

nebo komponentě smazána data tzv. degausserem (označováno též jako „magnetická pec“) nebo jiným odpovídajícím způsobem. Smazání dat na disku zajišťují zaměstnanci objednatele. Komponenty s nemagnetickým záznamem (např. SSD, Flash, paměti na řadičích apod.) objednatel nevrací a zajistí jejich bezpečnou likvidaci.

11. Zhotovitel se zavazuje, že v případě, že cena podpory zajišťovaná u výrobce bude zahrnuta v ceně díla podle čl. IV odst. 2 a z tohoto důvodu budou paušální ceny za podporu účtovány v symbolické výši, zajistí u výrobce možnost čerpání podpory přímo objednatelem, dojde-li k ukončení této smlouvy před uplynutím sjednané doby.

Článek VIII.
Smluvní pokuty, úrok z prodlení

1. V případě prodlení zhotovitele má objednatel právo požadovat smluvní pokutu:
   a) ve výši 5 000 Kč za každý den prodlení ve lhůtě dle čl. III odst. 1 písm. a);
   b) ve výši 5 000 Kč za každý den prodlení ve lhůtě dle čl. III odst. 1 písm. b);
   c) ve výši 2 000 Kč za každý den prodlení ve lhůtě dle čl. III odst. 1 písm. c);
   d) ve výši 1 000 Kč za každý den prodlení ve lhůtě dle čl. III odst. 1 písm. d).
2. V případě prodlení zhotovitele má objednatel právo požadovat smluvní pokutu:
   a) ve výši 5 000 Kč za každou hodinu prodlení ve lhůtě dle čl. VII odst. 2 písm. a);
   b) ve výši 1 000 Kč za každý pracovní den prodlení ve lhůtě dle čl. VII odst. 2 písm. b);
   c) ve výši 500 Kč za každou hodinu prodlení ve lhůtě pro zahájení odstraňování závady nebo neodůvodněného přerušení odstraňování závady dle čl. VII odst. 2 písm. c);
   d) ve výši 500 Kč za každou hodinu nedostupnosti prostředku pro předání požadavku dle čl. VII odst. 7.
3. V případě, že mezi dvěma odstávkami potřebnými pro aktualizaci firmware kteréhokoliv technického prostředku dodaného podle čl. I odst. 1 této smlouvy uplyne méně než 12 měsíců nebo doba jedné odstávky bude delší než 4 hodiny, je objednatel oprávněn požadovat po zhotoviteli smluvní pokutu ve výši 5 000 Kč za každý takový případ. Uvedené nezbavuje zhotovitele povinnosti takovou závadu odstranit v souladu s touto smlouvou ani splnit technické požadavky dle přílohy č. 4 této smlouvy. Uvedeným není dotčeno právo na odstoupení od smlouvy. Možnost uplatnění této smluvní pokuty vylučuje uplatnění smluvní pokuty podle odst. 4 za tutéž událost.
4. V případě, že se v průběhu provozu prokáže, že nebyl splněn některý z požadavků uvedených v příloze č. 4, vyjma případu dle odst. 5, má objednatel právo požadovat smluvní pokutu ve výši 10 % z ceny druhého dílčího plnění uvedené v čl. IV odst. 3, nejméně však 100 000 Kč, a to za každý případ nedodržení závazného požadavku. Uvedené nezbavuje zhotovitele povinnosti doplnit chybějící technický požadavek dle přílohy č. 4 této smlouvy. Uvedeným není dotčeno právo na odstoupení od smlouvy.
5. V případě, že se v průběhu provozu prokáže, že nebyl splněn požadavek „Kapacita“ uvedený v příloze č. 4, je objednatel oprávněn požadovat smluvní pokutu ve výši 20 000 Kč za každý den provozu až do splnění požadavku. Objednatel v této souvislosti výslovně upozorňuje na problematiku deduplikace a komprese. Uvedeným není dotčeno právo na odstoupení od smlouvy.
6. Objednatel upozorňuje zhotovitele, že odhad/výpočet splnění požadované kapacity (týká se zejména technologií s deduplikací nebo kompresí) bude stanoven 1 měsíc po předání

a převzetí třetího dílčího plnění a pak následně jeden rok po předání a převzetí prvního dílčího plnění. Výpočet bude proveden tak, že se z dodaných prostředků nástroji pro správu zjistí skutečné reálné zaplnění a prostředky DataProtector (příkaz omnirpt). Následně se provede lineární extrapolace pro požadovanou kapacitu uložení (požadavek „Kapacita“ dle přílohy č. 4). Splnění požadavku může být dále ověřeno kdykoliv později po dobu 5 let od předání a převzetí prvního dílčího plnění (např. při vysokém stupni zaplnění).

7. V případě prodlení zhotovitele s předložením dokladů o existenci pojistné smlouvy dle čl. VI odst. 6 této smlouvy je objednatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každý den prodlení.
8. V případě porušení závazku mlčenlivosti zhotovitele dle čl. XI je objednatel oprávněn požadovat smluvní pokutu ve výši 20 000 Kč, a to za každé takové porušení.
9. V případě prodlení s uhrazením daňového dokladu zaplatí objednatel zhotoviteli úrok z prodlení podle předpisů občanského práva.
10. Ujednáními o smluvní pokutě není dotčeno právo smluvních stran na náhradu škody.

Článek IX.
Odstoupení od smlouvy

1. Zhotovitel bere na vědomí, že pro objednatele je nezbytné, aby veškeré dodané technické a programové prostředky jako celek splňovaly funkční požadavky uvedené v příloze č. 4.
2. Pro účely náhrady škody v případě odstoupení se stanovuje cena práce každého ze zaměstnanců objednatele na implementaci ve výši 1 300 Kč/hod.
3. Objednatel je oprávněn odstoupit od smlouvy v případě, že:
   a) zhotovitel bude v prodlení s předáním kteréhokoliv (dílčího) plnění dle čl. III odst. 1 po dobu delší než 30 dnů,
   b) systém offline zálohování s implementovanými technickými a programovými prostředky podle čl. I odst. 1 této smlouvy nesplňuje některou/ý z požadovaných funkcí/požadavků uvedených v příloze č. 4,
   c) systém offline zálohování nesplňuje požadavek na nesmazatelnost a neměnnost dat,
   d) systém zálohování s implementovanými technickými a programovými prostředky podle čl. I odst. 1 této smlouvy nevykazuje některou z požadovaných hodnot podle přílohy č. 10, tabulky „Provedené testy“, nebo
   e) nebudou odstraněny vady uvedené v protokolu o předání a převzetí některého z dílčích plnění ani v dodatečné lhůtě v protokolu uvedené.
4. Objednatel je dále oprávněn odstoupit od smlouvy v případě, že se v rámci zkušebního provozu dle čl. V vyskytnou závady, které:
   a) zapříčiní přerušení zkušebního provozu na déle než 30 dnů,
   b) opakovaně zapříčiní opakování zkušebního provozu nebo jeho části, nebo
   c) byly uvedeny v protokolu o předání převzetí druhého dílčího plnění a byly i odstraněny v dodatečné lhůtě k tomu v protokolu uvedené, avšak projevily se znovu ve zkušebním provozu.
5. Objednatel je oprávněn odstoupit od smlouvy také tehdy, jestliže se během jakýchkoliv bezprostředně po sobě jdoucích 12 měsíců vyskytne na technických nebo programových prostředcích dodaných podle této smlouvy více jak 24 závad.

6. Zhotovitel je oprávněn odstoupit od smlouvy v případě prodlení objednatele s úhradou daňového dokladu, a to po dobu delší než 30 dnů.

Článek X.
Vlastnictví, nebezpečí škody na věci a licenční ujednání

1. Vlastnictví k technickým prostředkům a právo užívání programových prostředků dle této smlouvy přechází na objednatele dnem převzetí druhého dílčího plnění.
2. Dnem převzetí technických prostředků objednatelem do úschovy přechází nebezpečí škody na těchto prostředcích na objednatele.
3. Zhotovitel poskytuje objednateli nevýhradní, nepřevoditelnou a místně neomezenou licenci, a to na dobu trvání majetkových práv umožňující užívat programové prostředky, dodané dle této smlouvy, pouze pro vnitřní potřebu objednatele.
4. Licence podle odst. 3 je poskytována též pro dokumentaci podle čl. I odst. 2 písm. d).
5. Licence poskytnuté dle této smlouvy se vztahují i na veškeré poskytnuté aktualizace poskytnutých programových prostředků (tj. update / upgrade / patch / hotfix atd.).
6. Zhotovitel poskytuje objednateli nevýhradní, převoditelnou a místně neomezenou licenci na dobu trvání majetkových práv k realizačnímu projektu a realizační dokumentaci. Uvedené plnění nebo jeho části může dále objednatel sám nebo prostřednictvím třetí osoby měnit, upravovat, zpracovávat, spojovat s jiným (autorským) dílem / prvky či zařazovat do jiného (autorského) díla souborného.
7. Odměna za poskytnutí licencí je zahrnuta v ceně díla, resp. v cenách jednotlivých dílčích plnění.
8. Objednatel není povinen licence využít.
9. Zhotovitel prohlašuje, že práva, která touto smlouvou poskytuje, mu náleží bez jakéhokoliv omezení, a odpovídá za škodu, která by objednateli vznikla, pokud by toto prohlášení bylo nepravdivé.

Článek XI.
Mlčenlivost

1. Zhotovitel se zavazuje zajistit, že jeho pracovníci a pracovníci jeho poddodavatelů, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se u objednatele seznámí a které nejsou veřejně známy. Povinnost mlčenlivosti není časově omezena.

Článek XII.
Uveřejnění smlouvy a výše skutečně uhrazené ceny

1. Zhotovitel si je vědom zákonné povinnosti objednatele uveřejnit na svém profilu tuto smlouvu včetně všech jejích případných změn a dodatků a výši skutečně uhrazené ceny za plnění této smlouvy.
2. Profilem objednatele je elektronický nástroj, prostřednictvím kterého objednatel, jako veřejný zadavatel dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ“), uveřejňuje informace a dokumenty ke svým veřejným zakázkám způsobem, který umožňuje neomezený a přímý dálkový přístup, přičemž profilem objednatele v době uzavření této smlouvy je https://ezak.cnb.cz/.

3. Povinnost uveřejňování dle tohoto článku je objednateli uložena § 219 ZZVZ.
4. Uveřejňování bude prováděno dle ZZVZ a příslušného prováděcího předpisu k ZZVZ.

Článek XIII.
Závěrečná ustanovení

1. Smluvní strany si v souladu s ustanovením § 1992 občanského zákoníku sjednávají, že objednatel je oprávněn zrušit tuto smlouvu zaplacením odstupného ve výši 50 000 Kč na účet zhotovitele, a to kdykoli do akceptace realizační studie. Zrušení smlouvy je účinné zaplacením sjednaného odstupného na bankovní účet zhotovitele. Zaplacením odstupného zanikají všechna práva a povinnosti obou smluvních stran vyplývající z této smlouvy s výjimkou závazku mlčenlivosti zhotovitele.
2. Smlouva nabývá platnosti a účinnosti dnem podpisu oprávněnými zástupci obou smluvních stran.
3. Tato smlouva se v části poskytování podpory uzavírá na dobu neurčitou.
4. Smluvní strany berou na vědomí, že technické a programové prostředky (dodané podle této smlouvy i jiné) mohou být v jejích přílohách dále souhrnně nebo jednotlivě nazývány „zařízení“ dle příslušného kontextu přílohy.
5. Smlouva může být měněna a doplňována pouze formou písemných vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran, není-li ve smlouvě uvedeno jinak. Za písemnou formu nebude pro účel uvedený v tomto odstavci považována výměna e-mailových či jiných elektronických zpráv, není-li ve smlouvě uvedeno jinak.
6. Použije-li zhotovitel při své činnosti poddodavatele, nahradí škodu jím způsobenou stejně, jakoby ji způsobil sám.
7. Smlouva je sepsána v českém jazyce. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě bude probíhat v českém jazyce, nebude-li smluvními stranami v konkrétním případě dohodnuto jinak.
8. Závazkové vztahy touto smlouvou založené se řídí českým právním řádem, zejména zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.
9. Smluvní strany se dohodly, že případný spor, který vznikne z této smlouvy nebo v souvislosti s ní, bude rozhodován výlučně podle českého práva obecnými soudy v České republice.
10. Smlouva je vyhotovena ve třech stejnopisech, z nichž objednatel obdrží dvě a zhotovitel jedno vyhotovení.
11. Odpověď strany této smlouvy podle § 1740 odst. 3 občanského zákoníku s dodatkem nebo odchylkou není přijetím nabídky, ani když podstatně nemění podmínky nabídky.
12. Uplatnění domněnky doby dojití dle § 573 občanského zákoníku se vylučuje.

Přílohy:

- č. 1 – Specifikace technických a programových prostředků
- č. 2 – Kontakty pro poskytování technické podpory
- č. 3 – Popis prostředí objednatele
- č. 4 – Technická specifikace předmětu plnění
- č. 5 – Návrh technického řešení
- č. 6 – Obecná pravidla pro dodavatele v oblasti bezpečnosti IT

č. 7 – Bezpečnostní požadavky ČNB
č. 8 – Specifikace cen plnění
č. 9 – Významné součásti realizačního projektu
č. 10 – Protokol o zkušebním provozu
č. 11 – Obsah realizační dokumentace

V Praze dne: 15.2.2022

Za zhotovitele:

[redacted]

Ing. Lumír Bolek
jednatel

KLANI S.R.O.
ANT. STAŠKA 2027/77
140 00 PRAHA 4
IČO 24750075

V Praze dne: 16.2.2022

Za objednatele:

[redacted]

Ing. Milan Zirnsák
ředitel sekce informatiky

[redacted]

Ing. Zdeněk Virius
ředitel sekce správní

ČNB ČESKÁ NÁRODNÍ BANKA
Na Příkopě 28, 115 03 Praha 1
48

Příloha č. 1

Specifikace technických a programových prostředků

Specifikace technických prostředků a programových prostředků, které jsou nedílnou součástí technických prostředků

Název (popis)			Rozlišení HW/SW*)	Množství (u HW počet ks, u SW počet licenčních jednotek)
PowerProtect DD6900	G7D4V2B	Controller DD6900 NFS CIFS	HW	1
TLA Order	GVCURS5	Non TLA Order		
Enclosure	GKWTX75	SYSTEM DD6900 NFS CIFS		
SSD Drives	G6UQ751	DD 1.92TB internal Cache SSD		
Rack Factory Installed or Field Installed	GV5UGQ3	Field Installed No Rack		
Field Power Cords	G6WMF3K	PDU 1M Included		
Base Warranty	GW7DN83	Parts Only Warranty 12Months, 12 Month(s)		
Hardware Support Services	G13JEKW	ProSupport and 4Hr Mission Critical, 48 Month(s)		
Operating System	GDVBJ4N	DD OS 7.4=IA		
DPE Input Output Cards	GNPYHB0	DD 10GSFP IO MODULE NDC		
DPE Input Output Cards	G9L5TAC	DD 12G 4 port SAS HBA		
DPE Input Output Cards	G346OYT	DD 10GBASE-T IO MODULE 4Port Full Height		
DPE Input Output Cards	GB13EK6	DD 16GBIT FC IO MODULE 4PORT		
Transceivers	GJZ2YFW	XCVR 10GbE SR SFP		
SAS Cables	GAN3IHZ	DD 3M SAS HD FLEX		
Operating Environment Software License	GSUEGC6	LICENSE BASE DD OE =IA		
Software Support - Operating Environment	G198DK7	ProSupport Mission Critical Operating Environment Software Support Maintenance, 48 Month(s)		

PowerProtect DD DAE	G3KSRIT	DD DS60 SHELF Field	HW	1
TLA Order	GVCURS5	Non TLA Order		
DD Capacity Software	GK1ABU9	DD New Software 1TB Raw=CB		240
Software Support - DD Capacity	GE425RB	ProSupport Mission Critical DD New 1TB Software Support Maintenance, 48 Month(s)		240
DD Shelf License	G2LQTO3	DS60 4TB Active 1TB Raw=CB		240
Software Support - DD Shelf License	GITSQY0	ProSupport Mission Critical DD Raw DS60 4TB Active 1TB Sftwr Spt-Maint, 48 Month(s)		240
Rack Factory Installed or Field Installed	G4FWEJR	FIELD INSTALLED DAE		
External SSDs and Disk Packs	G80IQOM	HDD 12G DISK PK 15X4TB SAS FL DS60		
Base Warranty	GW7DN83	Parts Only Warranty 12Months, 12 Month(s)		
Hardware Support Services	G13JEKW	ProSupport and 4Hr Mission Critical, 48 Month(s)		
Keep Your Hard Drive or Component for Ent Services	GY01FXN	Keep Your Hard Drive For Enterprise, 48 Month(s)		
DPE Selection	GC0ZVOJ	DD6900 Selected		
PowerProtect DD DAE	G3KSRIT	DD DS60 SHELF Field	HW	1
TLA Order	GVCURS5	Non TLA Order		
DD Capacity Software	GK1ABU9	DD New Software 1TB Raw=CB		120
Software Support - DD Capacity	GE425RB	ProSupport Mission Critical DD New 1TB Software Support Maintenance, 48 Month(s)		120
DD Shelf License	G2LQTO3	DS60 4TB Active 1TB Raw=CB		120
Software Support - DD Shelf License	GITSQY0	ProSupport Mission Critical DD Raw DS60 4TB Active 1TB Sftwr Spt-Maint, 48 Month(s)		120
Rack Factory Installed or Field Installed	G4FWEJR	FIELD INSTALLED DAE		
External SSDs and Disk Packs	G80IQOM	HDD 12G DISK PK 15X4TB SAS FL DS60		
Base Warranty	GW7DN83	Parts Only Warranty 12Months, 12 Month(s)		
Hardware Support Services	G13JEKW	ProSupport and 4Hr Mission Critical, 48 Month(s)		
Keep Your Hard Drive or Component for Ent Services	GY01FXN	Keep Your Hard Drive For Enterprise, 48 Month(s)		
DPE Selection	GC0ZVOJ	DD6900 Selected		

HPE DP Unlimited Slots Library E-LTU	SW	1
HPE DP drive ext UNIX/NAS/SAN E-LTU	SW	2
HPE DP support - 48 Month(s)		

*) U položek technických prostředků uveďte „HW“.
U položek programových prostředků uveďte typ (jednotky) licencování např. „*kapacita-TB*“, „*na storage*“, „*na server*“, „*na počet připojených zařízení*“, „*na CPU*“, „*na uživatele*“ apod. Lze doplnit i textem pod tabulkou.

Příloha č. 2

Kontakty pro poskytování technické podpory

Kontaktní osoby objednatele:

případně telefonicky nejméně jedné kontaktní osobě objednatele

Kontaktní osoby/centrum zhotovitele:

Příloha č. 3

Popis prostředí objednatele

Obecné informace

V ČNB jsou v provozu dvě výpočetní střediska. Obě tato střediska jsou provozována systémem aktiv-aktiv, tj. v obou střediscích jsou zpracovávány různé informační systémy. Běžný uživatel není schopen rozlišit, ve kterém středisku je jeho požadavek zpracován. V případě potřeby (havárie, údržba atd.) je zpracování konkrétního informačního systému, který je umístěn na některém ze serverů geoclusteru, přesunuto na jiný uzel clusteru (s krátkým výpadkem zpracování).

Do prostředí geografických clusterů jsou umísťovány IS přímo podporující jednu nebo více kritických činností ČNB. Jiné IS se do tohoto prostředí umisťují jen výjimečně (např. z licenčních důvodů, striktního požadavku na shodnost akceptačního a provozního prostředí apod.).

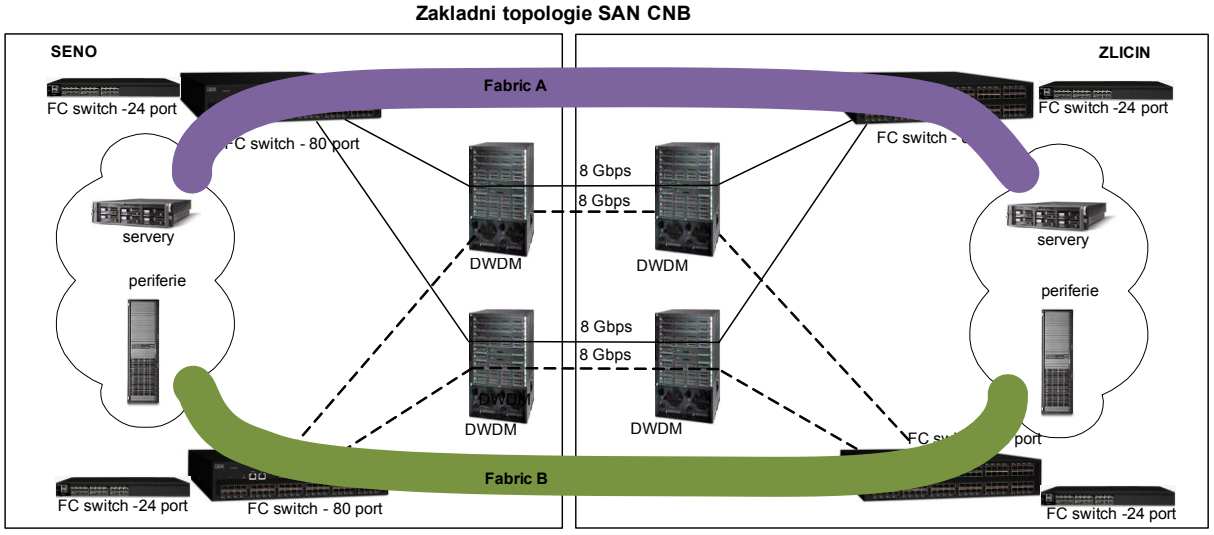
V případě havárie je výpadek ve zpracování (doba mezi zastavením IS a jeho nastartováním na jiném serveru) v délce do 5 minut pro ČNB akceptovatelný. V případě plánované údržby je nutné konkrétní dobu přesunu zpracování individuálně dohodnout se správcem příslušného IS.

Komunikační infrastruktura/SAN

Jedno výpočetní středisko je umístěno v budově ústředí v Praze 1 a druhé v Praze 5 – Zličín (dále také ZP). Obě střediska jsou plnohodnotně vybavena jak po stránce komunikační (LAN, SAN), tak i po stránce zpracování a uložení dat (servery, disková pole, VTL knihovny). Z kapacitního hlediska převažuje (počty serverů, objemy dat) objekt ústředí, ve kterém jsou také umístěny systémy nevyžadující zdvojení (méně významné IS, systémy pro testování a vývoj apod.).

Obě výpočetní střediska jsou propojena optickými vlákny (single mode) dvěma nezávislými trasami. Jedna z tras je dlouhá 22,0 km, druhá trasa je dlouhá 24,4 km. Obě trasy jsou rovnocenné z hlediska přenášených protokolů (TCP/IP, FC) a přibližně i objemu přenášených dat. Na obou koncích jsou umístěny multiplexory DWDM (technická specifikace viz dále v tabulce).

Obecné schéma zapojení SAN je v následujícím obrázku:



SAN je tvořena dvěma vzájemně oddělenými fabricy (Fabric A, Fabric B), každý z nich je tvořen dvěma FC switchi umístěnými v jiné lokalitě (v obrázku jsou prvky fabricu propojeny vždy stejným typem čáry). Každý z fabriců využívá obě optické komunikační trasy mezi objekty. Všechny prvky SAN (FC switche) jsou ve shodné HW a SW konfiguraci (viz dále v tabulce).

Páteřní optické rozvody v rámci objektu ústředí jsou 62,5 um, v objektu ZP Zličín jsou 50 um (typ vlákna OM3). Multimode páteřní optická kabeláž je zpravidla zakončena konektory typu SC na patch panelech v objektu ústředí. Ostatní kabeláž je zakončena konektory typu LC (patch panely v objektu ZP Zličín a prvky SAN v obou objektech).

Hardware	**verze OS**	**poznámka**	**poznámka**
FC switche CISCO MDS-9396T	FOS v7.2.1b	8-32 Gbit/s:	každý ze dvou fabriků má ISL 2x8 Gbit/s (trunk)
DWDM Cisco ONS 15454 – M6		vzdálenost cca 22, resp. 24 km, zapnuto šifrování	

Celková přenosová kapacita protokolu FC mezi objekty je 4 x 8 Gbit/s, celková přenosová kapacita protokolu Ethernet mezi objekty je 4 x 10 Gbit/s. Lokality jsou propojeny protokolem TCP/IP na úrovni L2 z hlediska rozhraní Ethernet.

Prostředí výpočetního střediska

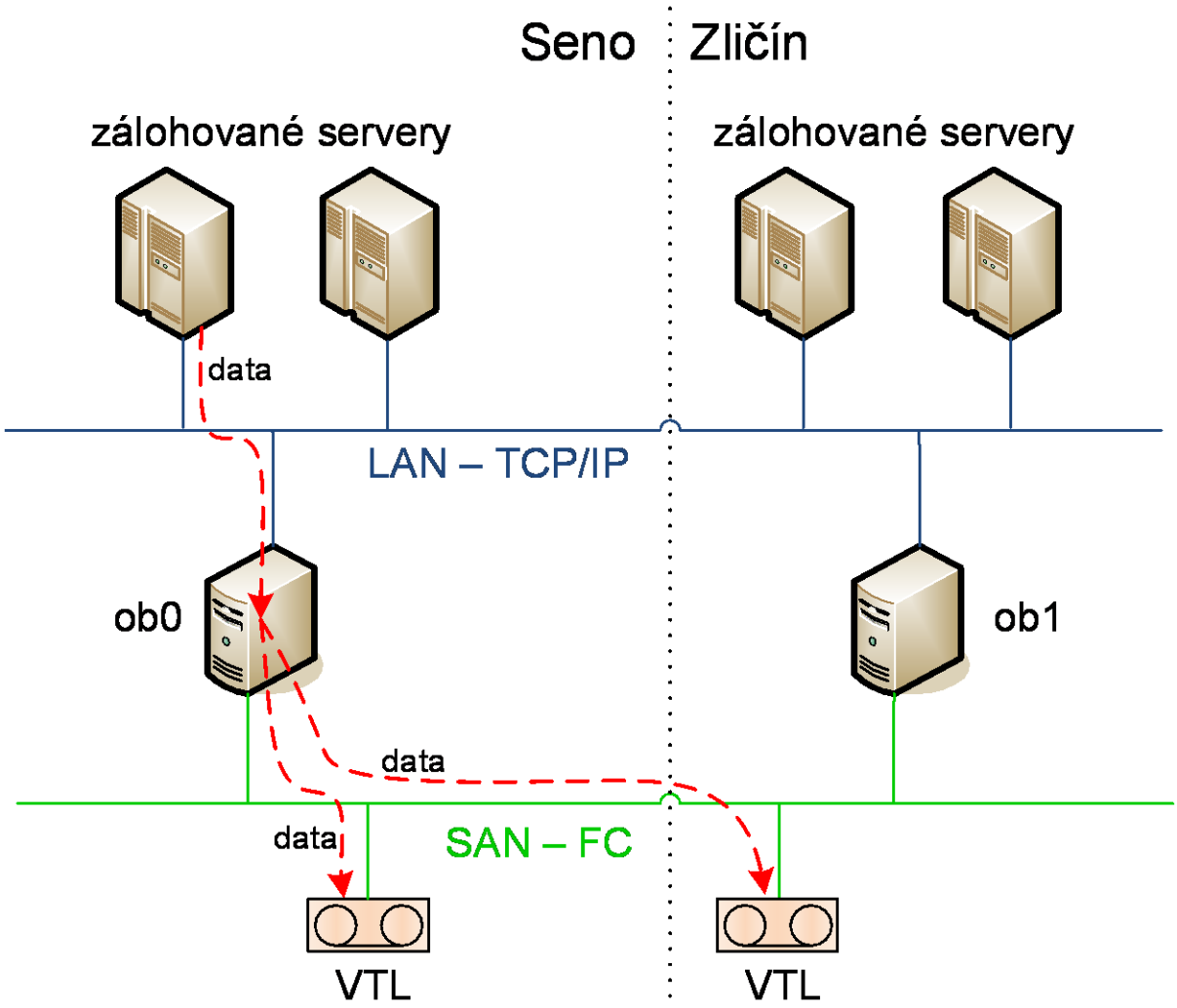
Výpočetní středisko je vybaveno:
- zdvojenou podlahou;
- redundantním systémem udržování provozního prostředí (teplota, vlhkost);
- napájením prostřednictvím redundantních UPS (zdvojené přívody do prostor výpočetních středisek, přepěťové ochrany, z rozvaděčů ke spotřebičům rozvod 230V). Do rozvaděčů jsou přívody 400V, ale pro připojení zařízení s 3-fázovým vstupem by byla nutná úprava rozvaděčů;
- požární signalizací;
- samozhášecím systémem na bázi inertního plynu;
- detekcí úniku kapalin ve zdvojené podlaze;
- zabezpečením proti neoprávněnému vstupu;
- vstupem do obou výpočetních středisek s maximální výškou 197 cm;
- transportní trasa do výpočetního střediska má omezení s ohledem na nosnost v transportní trase nebo rozměry transportní trasy. V objektu je transport možný až po 18 hod.

Současný stav zálohovacího systému

Zálohovací systém je tvořen:
- „cell managerem“ na platformě RedHat Linux 7 a SW Microficus DataProtector 10.70 nebo vyšším;
- **dvěma VTL knihovnami HPE StoreOnce 5650**. V každé fyzické VTL knihovně jsou nadefinovány 2 virtuální knihovny. Používány jsou emulace drivů LTO 4. ČNB má pro DataProtector licenční pokrytí pro 2x „Unlimited slots Library“+22x“SAN drive“ a dále 2x“10+1 TB Advanced Backup to disk“ (celkem 22 TB). Na každé fyzické knihovně jsou

tedy nedefinovány 2 virtuální knihovny. První knihovna je licencována slots+drive, druhá knihovna je licencována na kapacitu. Při kompresním (deduplikačním) poměru 13:1 je možné na druhou knihovnu uložit více než 140 TB zdrojových dat.

- Zálohovací systém je tvořen čtyřmi „drive servery“ (DP media agent). Dva z nich jsou totožné se servery, kde jsou provozovány cell managery a 2 jsou servery Windows 2016. Každý média agent má připojeny všechny drivy (jak ze "své" lokality tak i z druhé lokality). Zálohovaný server posílá data v rámci lokality media agentu prostřednictvím TCP/IP a ten prostřednictvím SAN zapisuje současně data do knihoven v obou lokalitách;
- zálohování je v provozu v režimu 24x7, odstávky na dobu do 2 hodin jsou možné i v běžné pracovní době;
- Windows Media agent zpravidla obsluhuje klienty s operačním systémem Windows, Linux cell obsluhuje zpravidla klienty s OS Linux;
- v současné době je celkový objem dat uložených do jedné knihovny cca 1,2 PB/měsíc.



Základní informace o objemem procházejících zálohovacím systémem. Zdůrazňujeme, že se jedná o hodnoty za listopad 2019:

Přehled podle cell managerů

Cell manager		
Denní objem cca GB	40 TB	Průměr do jedné knihovny (tj. bez mirroru) Z toho archivní redology databází cca 20%
Denní maximum	45 TB	
Denní počet session	2800	Z tohoto archivní redology databází cca 90%
Počet klientů	370	Zahrnuje i virtuální adresy v rámci clusterů
Počet transportu médií	122 000	
Největší záloha	13 TB	filesystém
Největší počet souborů v jedné záloze	50 milionů	7,5 TB
Největší rychlost	2 TB/hod	záloha Oracle DB

Ostatní informace

U zálohování je zanedbatelné množství zašifrovaných souborů; kompresená data (např. jpeg, zip, mpeg, ….) se vyskytují, ale jejich množství je problematicky odhadnutelné. Systém obsahuje velké množství dat, která se mění – typicky archivní redology databází.
Starší zařízení EMC DataDomain 2500 reportovalo průměrnou hodnotu deduplikace 1 : 13. Aktuální hodnota u HPE StoreOnce není známa, protože není dokončen převod všech dat.

Standardní systémové prostředí ČNB (základní informace)

Tato část informací je uvedena pro úplnost, aby zhotovitel měl v případě potřeby kompletní informace o prostředí ČNB.

Počítačová síť – interní standard technického a programového vybavení

Standardní technické komunikační vybavení:

- LAN – strukturovaná kabeláž pro připojení uživatelů umožňující připojení rychlostí minimálně 1000 Mbit/sec. Standardní provedení je metalické, optická vlákna jsou typem doplňkovým.
- Páteřní LAN – Gigabit Ethernet;
- aktivní síťové prvky – platforma CISCO, plně přepínaná síť;
- LAN, MAN, WAN – multiplexory typu WDM;
- Ethernet dle ISO 802.3 pro připojení uživatelských stanic;
- Protokol TCP/IP v4.

Příloha č. 4

Technická specifikace předmětu plnění

Terminologie

Cluster lokální - skupina zařízení (zpravidla serverů a diskových polí), která umožňuje zajistit obnovu zpracování v řádu jednotek minut po výpadku některé z komponent. Vzájemná vzdálenost zařízení od sebe může být do desítek metrů.

Cluster geografický/geocluster - obdoba lokálního clusteru s tím rozdílem, že tato technologie umožňuje kompletní obnovu zpracování ve fyzicky jiné lokalitě (vzdálenost desítky kilometrů). Data jsou v obou lokalitách.

IS (Informační systém/aplikace) - je funkční celek, který slouží k získávání, uchovávání, přenášení, zpracovávání a poskytování informací pomocí informačních technologií. Zahrnuje informační technologie, data, správu informačního systému a zaměstnance, kteří ji zajišťují, uživatele a vzájemné vazby mezi nimi.

MSCS (Microsoft Cluster Service) – SW dodávaný firmou Microsoft zajišťující funkci clusteru. Tento SW je součástí MS Windows Enterprise Edition.

Synchronní/Asynchronní přenos - pojmem synchronní přenos je označován typ přenosu, kdy odesilateli je doručeno potvrzení o zpracování jeho požadavku až v okamžiku dokončení zpracování (tím vzniká časové zpoždění). Naproti tomu asynchronní přenos považuje operaci za ukončenou v okamžiku ukončení odeslání požadavku bez ohledu na to, zda operace je již dokončena a bez ohledu na to, zda byla ukončena korektně.

ZP – záložní pracoviště ČNB v Praze-Zličín.

Backup Session – proces, který vytváří kopii dat na cílovém médiu

Restore session – proces, který obnovuje data z předchozí backup session na disk

Session – je backup session nebo restore session

1. **Vyžadované funkce a vlastnosti**:

Tato kapitola obsahuje informace potřebné pro návrh řešení.

Cílem **není** kompletní přepracování systému zálohování, ale rozšíření současného systému (2 sady dat) o třetí kopii, která bude chráněna proti neoprávněnému zásahu.

Obecně nejsou kladeny žádné požadavky na typ nabízené technologie. Požadavky jsou na úrovni funkčních a výkonnostních specifikací. Z technického hlediska je kladen důraz na kompatibilitu s navazujícími technologiemi, minimalizaci nároků na údržbu a správu nových zařízení.

Pokud v níže uvedené specifikaci vzniknou jakékoliv pochybnosti o významu textu, je potřeba význam zásadně vykládat v kontextu účelu dodávky, tj. maximální zajištěny ochrana dat, maximální rychlost obnovy dat po napadení/poškození **a současně zajištění maximální průchodnosti systému.**

V následující tabulce jsou uvedeny požadavky, které musí být zhotovitelem splněny. Vzhledem k tomu, že specifikace požadavků je na obecné úrovni (tj. nespecifikuje jednu konkrétní technologií), není možné všechny požadavky specifikovat zcela přesně.

Vzhledem k tomu, že zadání je obecné, bude v dalším textu slovem „drive“ nebo „drivy“ míněn buď skutečný drive magnetopáskové jednotky, virtuální drive virtuální knihovny nebo i diskový úložný prostor.

Obecné principy

	Popis	**KLARI**
Doba uložení	Zajištění ochrany uložených dat po dobu 30-60 dnů od okamžiku uložení. Tato doba musí být buď: - nastavitelná administrátorem jednotně pro všechna vstupní data. - Nastavitelná pro konkrétní ukládaný objekt. V tom případě musí existovat transparentní vazba na SW DataProtector, odkud bude tato informace (doba uložení) čerpána a musí být ekvivalentní s dobou uložení v DataProtectoru.	**ANO**, nastavitelná administrátorem jednotně pro všechna vstupní data
Neměnnost doby uložení	Systém (implementované řešení)	**ANO**, retention lock compliance Varianta b) je možná, ale není součástí nabídky

	a) neumožňuje pro zapsaná data zkrátit dobu uložení (dobu, po kterou jsou chráněna proti smazání a proti přepsání/změně) nebo je smazat nebo b) je nakonfigurované tak, že změna doby uložení je možná jen lokálně, tj. z panelu na zařízení nebo z konzole připojené na fyzický port zařízení, nebo z počítače zapojeného do samostatné sítě, která je součástí implementovaného řešení, a je zaznamenána do logů. Týká se i smazání dat. To se týká např. i možnosti administrátorů vybrat k zápisu výměnná média před tím, než uplyne doba uložení na nich zapsaných dat.	
Ochrana	**Data uložená** v systému musí být chráněna tak, že není možné je jakýmkoliv způsobem smazat, modifikovat, znepřístupnit nebo znevěrohodnit. Tato ochrana musí být aplikována na všechny možné přístupy k datům a to např. z pozice ukládání dat (vstupní interface pro data), managementu (administrátorský přístup), apod. Tento požadavek se týká způsobu (technologie) uložení dat a způsobu jejich správy (např. správa paritních skupin/RAID, filesystému apod.). Nepostačuje pouhé prokázání, že data byla/nebyla změněna (např. časovou značkou). Systém musí chránit před **jakýmikoliv** útoky prostřednictvím počítačové sítě, a to i např. včetně variant, že útočník získá několik administrátorských hesel apod. Není potřeba zohlednit fyzickou ochranu zařízení, naopak je toto možné využít jako součást ochrany (např. ovládání zařízení pouze z čelního panelu nebo prostřednictvím speciálního portu, ke kterému se připojí notebook apod.). Smazání dat nesmí být možné ani prostřednictvím výrobce (např. různé typy speciálních hesel platných po omezenou dobu).	**ANO,** SAN není LAN a sama o sobě by měla být bezpečná.

	Zadavatel připouští jedinou výjimku a to je možnost poškození sady dat uložených v systému v posledních 24 hodinách. Zadavatel tedy připouští, že v rámci ukládání do systému může vznikat pracovní kopie dat (např. disková cache), která nemá tak vysoké zabezpečení. Podmínkou je však přesun těchto dat do „zabezpečené“ části a to nejpozději do 24 hod od prvotního uložení konkrétního objektu (dat). V případě napadení (např. ransomware) ČNB zajistí obnovu provozu serveru s DataProtector, SAN a LAN. Dodaný systém musí útoku odolat. Jiné komponenty ČNB nesmí být potřeba obnovovat (např. současné kapacity StoreOnce byť jen do úrovně konfigurace virtuálních knihoven). Cílem je minimalizovat čas potřebný k zahájení obnovy dat uložených v „offline zálohování“ Řešení tedy nemůže být založeno na pravidelném vyjímání pásek operátorem (není obsluha během víkendů), ale může být **např.** založeno na: - pravidelném snapshotu - přesunu médií do zabezpečené „mezi oblasti“, odkud je může operátor např. 1xtýdně transportovat do trezoru	
Obnova katalogu	V případě poškození databáze (IDB) zálohovacího systému DataProtector musí existovat možnost načtení uložených dat (catalog) z dodaného zařízení. Načtení katalogu dat uložených za jeden den nesmí být delší než 10 hodin.	**ANO**, doba záleží na výkonu primární zálohovací infrastruktury
Konfigurace a performance	Provádění změn konfigurace a sledování zátěže zařízení (performance) je možné řešit zapojením např. PC umístěného přímo u zařízení (např. export csv dat apod.), tj. port pro konfiguraci nebude trvale zapojen.	**ANO**, konkrétní způsob řešení bude připraven v rámci realizačního projektu.
Typ provozu	Zařízení bude pracovat v režimu 24x7, ale (fyzická) obsluha pro pravidelné aktivity (netýká se havárií) je zajištěna jen v pracovní dny (viz také požadavek Ochrana).	**ANO**
Řízení přístupu	přístup k datům (možnost obnovit data) musí mít pouze pracovníci, kterým byla výslovně přidělena příslušná role.	**ANO**

Řízení oprávnění k administraci	Možnost spravovat řešení (tj. především určovat jaká data budou zálohována a kdy, jak dlouho budou uložena apod.), musí mít pouze pracovníci, kterým byla výslovně přidělena příslušná role.	**ANO**, řízení přístupu je jednou základní vlastností řešení
Operátorské požadavky	Požadavky na operátorskou obsluhu maximálně v rozsahu 1 hod /pracovní den	**ANO**
Reporting chyb	Zařízení musí nějakým způsobem zajistit informování administrátorů o svém stavu. Způsob informování o chybách je na dodavateli, ale přes tento kanál nesmí být možné jakkoliv data ovlivnit nebo smazat (a to např. i smazáním/poškozením základního filesystému), ale musí být zajištěno informování alespoň 1x za den bez nutnosti fyzické návštěvy zařízení. Splnění požadavku je možné i formou předávání logů do systému SIEM ČNB (viz. Zaznamenávání událostí formou logů II). V tom případě musí dodavatel specifikovat algoritmus, jak ze zaslaných logů identifikovat potřebné informace.	**ANO**, emaily, SMS atd…, konkrétní způsob řešení bude připraven v rámci realizačního projektu.
Zaznamenávání událostí formou logů	Systém vytváří záznamy o událostech (logy), alespoň a) úspěšné i neúspěšné přihlašování a odhlašování ke všem účtům, b) činnosti provedené administrátory, zejména změna doby uložení a/nebo smazání médií nebo dat, c) úspěšné i neúspěšné manipulace s účty, oprávněními a právy, d) neprovedení činností v důsledku nedostatku přístupových práv a oprávnění, e) činností uživatelů, které mohou mít vliv na bezpečnost informačního systému, f) zahájení a ukončení činností technických aktiv, g) kritická i chybová hlášení technických aktiv, h) přístupy k záznamům o událostech, pokusy o manipulaci se záznamy o událostech a změny nastavení nástroje pro zaznamenávání činností, Každý auditní záznam musí obsahovat minimálně: a) datum a čas včetně specifikace časového pásma s přesností na sekundy, b) typ činnosti, c) identifikaci technického aktiva, které činnost zaznamenalo,	**ANO,** všechny požadavky jsou podporovány

	d) jednoznačnou identifikaci účtu, pod kterým byla činnost provedena, e) jednoznačnou síťovou identifikaci zařízení původce, f) úspěšnost nebo neúspěšnost činnosti.	
Zaznamenávání událostí formou logů II	Systém zajišťuje: a) automatické posílání logů do systému SIEM ČNB, např. syslog (syslog UDP/514 případně TCP, nejlépe formát CEF) nebo b) uložení logů po dobu alespoň 18 měsíců, ochranu logů proti smazání a možnost logy přenést (exportovat) na lokálně připojené zařízení. Přes tento kanál nesmí být možné jakkoliv uložená data ovlivnit nebo smazat.	**ANO**, automatické posílání logů do systému typu SIEM je podporováno, ale implementace není součástí nabídky. Uložení logů na požadovanou dobu (i delší) není problém
Autentizace administrátorů	Před umožněním administrace musí být uživatel autentizován a autorizován. K žádné části systému není možné získat přístup s využitím autentizačních informací (hesel, kryptografických klíčů apod.), které není možné změnit. Tj. systém neobsahuje „hardcoded“ hesla, „maintenance backdooor“ apod. Autentizace je založena na a) vícefaktorové autentizaci s nejméně dvěma různými typy faktorů, nebo b) autentizaci heslem. Při autentizaci heslem systém zajišťuje, že heslo - musí mít alespoň 12 znaků. - musí splňovat alespoň tři z následujících požadavků: malé písmeno, velké písmeno, číslici, nealfanumerický znak. **Vítané vlastnosti** (zadavatel povinně nepožaduje) - nastavitelná doba platnosti hesla; - automatické zablokování účtu po 15 dnech od vypršení lhůty pro změnu hesla. Přístup lze umožnit pouze pro změnu hesla; - minimální doba platnosti hesla 1 den nebo nastavitelná,	**ANO**, všechny požadavky jsou podporovány, vícefaktorovou autentifikaci nedoporučujeme, síla a doba platnosti hesla jsou konfigurovatelné Konkrétní způsob řešení bude připraven v rámci realizačního projektu v souladu s interními předpisy ČNB

	- mechanismus proti hádání hesel, např. po stanoveném počtu (nastavitelném nebo fixním) neúspěšných zadáních hesla se uživatelský účet zablokuje (na určitou dobu anebo do manuálního odblokování jiným administrátorem) nebo zvyšování prodlevy mezi jednotlivými pokusy. - nemožnost opětovného použití dříve používaných hesel s pamětí alespoň 12 předchozích hesel, - nemožnost zvolit si nejčastěji používaná hesla anebo tvořit hesla na základě mnohonásobně opakujících se znaků, přihlašovacího jména, e-mailu, názvu systému apod.	
Ochrana autentizačních informací	Heslo není v systému uloženo nebo přenášeno v nechráněné podobě.	**ANO**, není.
Princip oddělení povinností	Jsou dokumentovány role, které nesmí mít jeden uživatel současně, a výskyt kolizí je a) vyloučen technickým řešením nebo b) možné kontrolovat pomocí nástrojů pro reportování rolí přidělených uživatelům.	**ANO**, v případě, že ČNB využívá biometrické identifikační nástroje. Rozhodně je možné kontrolovat role pomocí nástrojů pro reportování rolí přidělených uživatelům.
Kryptografická ochrana přenášených dat	Pokud systém přenáší autentizační informace nebo administrátorské příkazy po síti, která není součástí dodaného řešení, musí být tato komunikace kryptograficky chráněna proti změně a odposlechu. Přitom: Jsou používány aktuálně odolné kryptografické algoritmy, schémata a protokoly. Jsou zohledněna doporučení v oblasti kryptografických prostředků vydaná NÚKIB, zveřejněná na jeho internetových stránkách. (v dubnu 2020 https://www.govcert.cz/cs/doporuceni-v-oblasti-kryptografickych-prostredku/) Systémy správy šifrovacích klíčů musí: - být v maximální možné míře automatizované a musí být minimalizována možnost úniku klíče. - Soukromé a symetrické klíče musí být uchovávány v tajnosti.	**ANO,** autentizační nebo administrátorské informace je možné kryptovat ale i přenášet po dedikované VLAN Konkrétní způsob řešení bude připraven v rámci realizačního projektu v souladu s interními předpisy ČNB

	- Soukromé a symetrické klíče, které jsou přenášeny, mohou být bezpečně předány pouze ověřeným stranám prostřednictvím odpovídajících protokolů a algoritmů. - Klíče odstraněné z paměťového zařízení musí být vymazány tak, aby je nebylo možné běžně dostupnými prostředky obnovit. Pro zabezpečení http spojení je použit protokol TLS 1.1 nebo vyšší, přičemž preferován je protokol TLS 1.2.	
Ochrana výměnných médií	Pokud jsou použita výměnná média (např. pásky), systém zaznamenává jejich vyjmutí a vložení.	Není součástí řešení
Oddělení	Systém (implementované řešení) c) neumožňuje pro zapsaná data zkrátit dobu uložení (dobu, po kterou jsou chráněna proti smazání a proti přepsání/změně) nebo d) je nakonfigurované tak, že změna doby uložení je možná jen lokálně, tj. z panelu na zařízení nebo z konzole připojené na fyzický port zařízení, nebo z počítače zapojeného do samostatné sítě, která je součástí implementovaného řešení, a je zaznamenána do logů. To se týká např. i možnosti administrátorů vybrat k zápisu výměnná média před tím, než uplyne doba uložení na nich zapsaných dat.	ANO, obě varianty jsou možné Konkrétní způsob řešení bude připraven v rámci realizačního projektu v souladu s interními předpisy ČNB

Technické požadavky:

Požadavek	**Popis**	**Poznámka/zdůvodnění**	**KLARI**
Kompatibilita	Zajištění kompatibility s DataProtector minimálně pro verzi 10.70	Pro dodané zařízení musí být zajištěna kompatibilita se stávajícím zálohovacím	ANO

		systémem-Microfocus „Data Protector 10.x Device Support Matrix“	
	Zajištění kompatibility a připojenými servery, se SAN a dalšími komponentami provozního prostředí ČNB (viz příloha č. 3).	Zařízení musí být kompatibilní se stávající infrastrukturou.	**ANO**
Kapacita	Je požadován úložný prostor pro minimálně 4000 TiB **klientských** dat. Uvedený odhad je čistý objem dat z klientů bez jakékoliv komprese nebo deduplikace. V uvedených 4000 TB není zahrnuto jakékoliv zabezpečení dat v případě použití diskového prostoru. Stanovení úrovně zabezpečení je na zhotoviteli. Objednatel však nepřipouští provoz diskového úložiště bez zabezpečení (RAID 0) a bez použití spare disků (v množství dle doporučení výrobce, minimálně však v množství po pokrytí výpadku 1 ks libovolného dodaného disku, na kterém budou uložena data nebo metadata). Pozn: 1 KiB=1024 byte, 1 MiB=1024 KiB, …	V případě použití zabezpečení RAID x, komprese nebo deduplikace musí být výpočtem doloženo, že bude dosaženo požadované kapacity - viz také požadavek „Deduplikace a komprese“ Výpočet pak bude kontrolován na reálných datech ČNB. Smluvní pokuty stanovené za porušení požadavku nebo jeho části nebrání objednateli označit plnění nesplňující tento požadavek za porušení smlouvy se všemi z toho plynoucímu důsledky. Nedodržení tohoto požadavku bude považováno za závadu dle smlouvy včetně všech následků z toho plynoucích, tj. včetně povinnosti zhotovitele tuto vadu na své náklady odstranit.	**ANO**, nabízené zařízení má 1,3x lepší deduplikační poměr než zařízení DD2500 Vzhledem k uvedenému deduplikačnímu poměru na datech ČNB je nabízená kapacita plně dostačující.
	Požadovaný „Výkonnost“ musí být dodržen pro celou dodávanou kapacitu, tj. při libovolném zaplnění knihovny (vč. zaplnění nad 95%) z požadovaných 4000TB musí být stále dosahováno požadovaného výkonu.	Smluvní pokuty stanovené za porušení požadavku nebo jeho části nebrání objednateli označit plnění nesplňující tento požadavek za porušení smlouvy se všemi z toho plynoucímu důsledky. Nedodržení tohoto požadavku bude považováno za závadu dle smlouvy včetně všech následků	**ANO**, viz výše

		z toho plynoucích, tj. včetně povinnosti zhotovitele tuto vadu na své náklady odstranit.	
Výkonnost	Systém musí být začleněn do současného komplexu, kdy jsou využívány všechny licence (drivové i kapacitní). Vytvoření třetí (nesmazatelné) kopie nesmí výkonnostně omezovat současné zálohy. Systém musí umožňovat běh minimálně 20 paralelních session (backup nebo restore) každá s přiděleným jedním drivem v každé z lokalit současně.	Pokud bude probíhat vytváření 3. offline kopie současně s běžnou zálohou, musí zařízení umožnit běh minimálně 20 záloh, kde bude každé záloze přidělen jeden drive. Toto se netýká vytváření kopií dat „post-procesingem“, pokud ten splňuje ostatní výkonové parametry. Obecně je možné řešení vytváření 3.kopie dat současně s prvními dvěma nebo vytváření kopie až později. Maximálně však 24 hodin po provedení zálohy. Všechny způsoby musí být zajištěny licenčně.	**ANO**, vytvoření 3.nesmazatelné kopie musí být vytvořena po ukončení primárního zálohováni. 3.kopie bude vytvořena jako lokální klon primární zálohy v jedné lokalitě.
	Celkový výkon pro zálohování (uložení do knihovny) požadovaný pro dodávaná zařízení je minimálně 2000 MB/s Pro jednotlivý stream (drive) je požadován výkon minimálně 400 MB/s		ANO, výkon zařízení je vyšší.
	Denní objem minimálně 60 TB/den Minimálně 100 miliónů souborů/den Průchodnost minimálně 2 GB/s, jeden stream minimálně 400 MB/s při záloze. Při obnově minimálně 75% těchto hodnot. Obnova dat přímo z prostředí DataProtector = uvnitř zařízení může probíhat nějaký typ tearingu (přesunu dat mezi vrstvami s různou výkonností), ale musí být pro DataProtector transparentní. Výkonnost jednotlivých vrstev však musí být dimenzována tak, aby i obnova starších záloh (např. 14 dnů) splňovala podmínky uvedené výše		ANO, nabízené zařízení násobně překračuje požadované hodnoty

	Restore nesmí být horší než 75% výkonu požadovaného pro zálohu.		**ANO**
	Navržené řešení nesmí prodloužit současné zálohy (např. při cca 3000 zálohách/den bude mít dlouhý mount/dismount média významný dopad do celkové doby zálohování).		**ANO**, navržené řešení nemá dopad na primární zálohy
	Drivy musí být rovnocenné z hlediska své výkonnosti a z hlediska přístupu k médiím	Všechny drivy musí mít přístup k médiím ve stejném rozsahu, tj. vyhrazení určitých médií pro použití v konkrétním drivu nesmí být obecným pravidlem, které nelze zrušit.	**ANO**
Zapojení do struktur ČNB	Zařízení je možné zapojit do struktur ČNB těmito interface: - LAN Ethernet 10 Gbit/s (maximálně 4 porty), IPv4 - LAN Ethernet 1 Gbit/s (maximálně 4 porty) - FC 32 GBit/s (maximálně 4 porty) Viz popis prostředí ČNB		**ANO**, nabízené interface jsou dostatečné, pro datové přenosy budou použity 4FC porty
Způsob připojení a spolehlivost	Podle způsobu realizace může jít o standardní knihovnu/VTL nebo např. protokol S3. Připojení drivů je požadováno protokolem FibreChannel (FC) s rychlostí 16/32 Gbit/s. Počet portů musí být minimálně 4 (=2 do každého fabricu SAN) a maximálně 8. Zařízení musí být připojitelné prostřednictvím LAN nebo SAN k serverům (Media agent) v obou lokalitách ČNB.		**ANO**, všechny požadavky na připojení a spolehlivost nabízené řešení splňuje

	Pro potřeby řízení je možné použít protokol TCP/IP.		**ANO**, všechny požadavky na připojení a spolehlivost nabízené řešení splňuje
	Zařízení musí umožňovat výměnu vadných komponent za provozu bez nutnosti odstávky. Navržené řešení musí být spolehlivostí konstruováno pro provoz 24x7 a musí minimalizovat potřebu odstávek, konkrétně tak: - Pro upgrade firmware je povolena odstávka na nejvýše 4 hodiny 1x za každých 12 bezprostředně po sobě jdoucích měsíců; - Zařízení nesmí vykázat více než 12 závad na všech svých součástech dohromady (všech dodaných technických a programových prostředcích) za každých 12 bezprostředně po sobě jdoucích měsíců. Pokud běží jakákoliv interní údržba (typicky reklamace uvolněného prostoru, reorganizace volných prostor na disku apod), pak její režie musí být nad požadovanými parametry kapacity a výkonnosti (Backup i restore)	Na straně ČNB vznikají náklady při časté poruchovosti nebo vynucených odstávkách. Zhotovitel by tedy měl zvážit kvalitu nabízeného řešení. Smluvní pokuty stanovené za porušení některých částí požadavku nebrání objednateli označit plnění nesplňující tento požadavek za porušení smlouvy se všemi z toho plynoucímu důsledky. Nedodržení tohoto požadavku bude považováno za závadu dle smlouvy včetně všech následků z toho plynoucích, tj. včetně povinnosti zhotovitele tuto vadu na své náklady odstranit.	**ANO**, všechny požadavky na připojení a spolehlivost nabízené řešení splňuje
	Zařízení musí být schopno uchovat uložené informace i v případě výpadku napájení (non-volatile) a samozřejmě nesmí při výpadku napájení data poškodit (maximálně smí být nedostupné médium nadefinované v DataProtectoru, se kterým se právě pracovalo).		**ANO**, všechny požadavky na připojení a spolehlivost nabízené řešení splňuje

	Pro potřeby identifikace zařízení je požadována identifikace jednotlivých drivů (např. přes sériové číslo nebo WWN) prostředky DataProtector (např. příkazem devbra –dev).	Při větším počtu drivů a cest k nim musí být jednotlivé drivy nějakým způsobem možné identifikovat. Tento požadavek se logicky netýká řešení založeného čistě na diskovém prostoru.	**ANO**, všechny požadavky na připojení a spolehlivost nabízené řešení splňuje
Zabezpečení dat-kopie dat	Požadavky na „zabezpečení dat-kopie dat“ **nejsou** zahrnuty v požadavcích „výkonnost“, protože není známa technologie, jakou se budou kopie dat vytvářet. Výslovně upozorňujeme na potřebu zohlednění potřeby větší hrubé kapacity při použití disků (využití RAID-<n>), výkonnostní kapacity pro kontrolu uložených dat, reklamaci prostoru (např. deduplikace) apod.	Výkonnostní požadavky na vytvoření kopie dat musí být zohledněny v návrhu řešení a musí odpovídat navrženému způsobu realizace.	**ANO**, nabízené řešení ČNB zná a splňuje všechny požadavky
	Systém musí provádět automatickou kontrolu čitelnosti dat (buď automaticky, nebo přes načasovanou úlohu), tj. v době nižší zátěže musí probíhat automatická kontrola čitelnosti stop/sektorů na discích.		**ANO,** nabízené řešení ČNB zná a splňuje všechny požadavky
Implementace řešení	V rámci implementace musí zhotovitel navrhnout způsob implementace nového řešení do prostředí objednatele a integraci se zálohovacím systémem DataProtector. Náhrada SW DataProtector je vyloučena.		**ANO**, Konkrétní způsob řešení bude přípraven v rámci realizačního projektu v souladu s interními předpisy ČNB
Deduplikace a komprese	V případě, že bude navržena technologie deduplikace dat, musí být toto řešení na nejvyšším stupni zabezpečení. **Musí být garantována 100% spolehlivost ve smyslu neměnnosti dat.**	Spolehlivost systému je v ČNB významná. Není přípustné, aby po případné obnově byl např. na některém účtu jiný zůstatek. Objednatel nezná dodávanou technologii a nemůže proto stanovovat deduplikační poměr. Po několikaletém provozu zařízení EMC	**ANO,** nabízené řešení ČNB zná a splňuje všechny požadavky

	Výkonnost deduplikčního systému musí být dostatečně dimenzována. Provádět deduplikaci na klientské straně objednatel nepřipouští (zátěž klienta).	DD2500 může objednatel pouze konstatovat, že je zde dosahováno deduplikančího poměru 13:1. Smluvní pokuty stanovené za porušení některých částí požadavku nebrání objednateli označit plnění nesplňující tento požadavek za porušení smlouvy se všemi z toho plynoucímu důsledky. Nedodržení tohoto požadavku bude považováno za závadu dle smlouvy včetně všech následků z toho plynoucích, tj. včetně povinnosti zhotovitele tuto vadu na své náklady odstranit.	
	Komprese na úrovni dodaných zálohovacích zařízení je přípustná jak na úrovni HW, tak na úrovni SW. Její režie však musí být zahrnuta v odhadech propustnosti a výkonnosti.	Komprese je přípustná na úrovni dodávaných zařízení. Není přípustné přenést kompresi na klienty zálohování nebo media agenty.	**ANO,** nabízené řešení ČNB zná a splňuje všechny požadavky
Licence	Zhotovitel dodá veškeré licence spojené s provozem dodávaného zařízení tak, aby byl v souladu s podmínkami výrobce dodávaného zařízení a současně, aby vyhovoval licenčním podmínkám HP DataProtector verze minimálně 10.70	Pokud v době dodávky budou jiné licenční podmínky pro různé verze DataProtector, musí být součástí dodávky licence pro zajištění provozu v obou verzích. Upozorňujeme také na fakt, že u virtualizovaných technologií mohou sice být neomezené počty knihoven, drivů a médií, ale na straně DataProtector je nutné odpovídající licencování.	Potřebné licence Microfocus Dataprotector pro vytvoření 3.kopie zálohy jsou součástí nabízeného řešení.
Kompatibilita s prostředím ČNB	Navržené řešení musí dodržovat standardy uvedené v části „Popis současného stavu a infrastruktury ČNB“.		Prostředí ČNB známe, navržené řešení je respektuje.

	Pokud bude mít dodané zařízení v sobě integrovány komponenty, které nedodržují výše uvedené standardy, je to možné pouze za předpokladu: - že daná komponenta je bezúdržbová ze strany ČNB; - že budou dodrženy minimálně komunikační a bezpečnostní standardy (pokud bude nutné komponentu zapojit do LAN/SAN); - zhotovitel zajistí na své náklady pravidelnou instalaci patches minimálně 2x ročně.		
Hmotnost	Dodávané technické prostředky musí být umístitelné ve výpočetních střediscích ČNB. Bez dalších specifických statických výpočtů je možné do každého ze středisek umístit do standardního 19“ stojanu ČNB. Maximální velikost je 25U/stojan, hmotnost nesmí překročit 350 kg/stojan. V lokalitě lze využít maximálně 2 stojany vzdáleno od sebe cca 2 metry. Zařízení překračující uvedené parametry nesmí být nabízena. V objektu ústředí je realizace výpočetního střediska formou „teplá ulička“ a musí tedy být použity stojany ČNB zaintegrované do uličky.¨ Je možné buď využít maximálně 25U v jednom stojanu.		**ANO**
Rozměry	Transportní trasy umožňují bezproblémovou dopravu zařízení s těmito parametry: maximální výška 195 cm, maximální základna 90 cm x 110 cm.	Požadavek vychází z možností transportních tras do očekávaného umístění.	**ANO**

	Zařízení větších rozměrů nesmí být nabízena.		
Napájení	Požadováno zdvojené, 1 fázové 230 V	Ve výpočetních střediscích ČNB jsou rozvaděče připraveny pro připojení systémů s 1 fázovým napájením.	**ANO**
Konfigurační změny	Zařízení musí umožňovat definovat drivy, média a knihovny na uživatelské/administrátorské úrovni. Je požadována možnost zálohování konfigurace zařízení.	Pro pružné a efektivní využití je nezbytné zajistit možnost konfiguračních změn na úrovni zaměstnanců objednatele.	**ANO**
Vzdálený přístup	Přístup servisní organizace ze sítě mimo ČNB je zakázán.		**ANO**, respektujeme

Příloha č. 5

Návrh technického řešení

Nabízené řešení tvoří Power Protect DataDomain 6900 a licence Microfocus DataProtector.

Popis nabízených technických a programových prostředků (může být i přílohou jen v elektronické formě a může být i v anglickém jazyce)

Nabízené řešení tvoří Power Protect DataDomain 6900 a licence Microfocus DataProtector.

Popis začlenění do struktur ČNB na fyzické úrovni (počty potřebných portů, jejich parametry)

Pro přenosy dat navrhujeme použít 4FC porty (2 v každém fabricu) a pro Management Ethernet. Vzhledem ke zvýšeným požadavkům na zabezpečení navrhujeme využití VLAN. Konkrétní způsob řešení bude připraven v rámci realizačního projektu v souladu s interními předpisy ČNB

Popis začlenění do struktur ČNB na logické úrovni, kdo s kým komunikuje (jak mezi dodávanými komponentami tak i komunikace ke komponentám ČNB), na jakých protokolech-TCP/IP nebo FC nebo jiné-uvést jaké

Vytvoření 3.kopie je řízeno na úrovní zálohovacího software. Po ukončení primárních záloh je spuštěno klonování zálohy na lokální úrovni. Všechny datové přenosy probíhají plnou rychlostí na SAN (protokol FC), řízení po síti na protokolech TCP/IP

Popis zajištění vytváření 3.kopie dat

viz výše

Popis zabezpečení proti neoprávněné změně uložených dat

viz přiložená dokumentace Retention lock compliance.

Pokud je replikace na úrovni dodaných zařízení, tak i způsob „zviditelnění“ těchto kopií DataProtectoru (detailně musí být způsob „zviditelnění“ uveden v případě kopie na úrovni dodaných zařízení bez kooperace s DataProtector)

Vytvoření 3.zalohy zálohovacím softwarem jednoznačně zajišťuje přístupnost 3.kopie z Microfocus Dataprotectoru

Navržené počty médií a zdůvodnění uvedeného počtu (pouze v případě fyzických médií)

Využíváme virtuální technologii.

Informace o způsobu zabezpečení dat a informace a dosažení požadované kapacity (doložené výpočtem)

Kalkulace vychází z informací v zadávací dokumentaci a datových listech výrobce.

V zadávací dokumentaci je uveden deduplikační poměr 1:13 na reálných datech ČNB na zařízeni DD2500 (předchozí generace zařízeni DD6900 nabízeného v řešení). U DD2500 je výrobcem uváděn deduplikační poměr 1:50 na zkušebním vzorku dat. Skutečně dosažený deduplikační poměr je tedy přibližně 3,8 krát menší.

U zařízení DD6900 je udáván deduplikační poměr 1:65 (vylepšení deduplikačniho poměru 1,3 krát) a logická kapacita 18,7 PB. Při stejném poměru mezi výrobcem udávaným deduplikačním poměru a reálně dosaženém na datech banky je tedy možno uložit 18,7 : 3,8=4,9PB.

Kontrola vypočtu

Fyzická čista kapacita zařízeni je 288TB.

Očekávaný deduplikační poměr je 13x1,3=16,9. 288x16,9=4867TB, to je přibližně 4,9 PB.

Ze zkušeností víme, že výkon zařízení není nijak omezen do zaplnění na 90% a jen mírně se projevuje do 95% zaplnění zařízení. Je tedy možno počítat s reálnou kapacitou 4,4PB při 90% zaplnění. To s rezervou splňuje požadavek na 4000TiB.

Zařízení DD6900 má podle výrobce za hodinu uložit 15TB dat. To je více než 4GB/s. Tuto propustnost dosáhneme na dvou portech FC 16Gb, je tedy s rezervou zaručen požadovaný výkon 2GB/s. Vzhledem k tomu že třetí kopie zálohy je klonem primární zálohy vytvořeným lokálně po ukončení primární zálohy (konsolidovaná data), je velmi pravděpodobné že ani zálohovací systém nebude významně omezovat přenosovou rychlost.

Informace o dosažení požadované propustnosti

viz výše a dokumentace

Informace o dodávaných licencích programových prostředků přímo souvisejících s dodávanými technickými prostředky. Informace o licencích souvisejících s DataProtector a potvrzení/prohlášení, že licence jsou dostačující pro provoz. Současně je požadována informace o způsobu zajištění licencování v přechodném období (souběh starého a nového řešení). (Zadavatel upozorňuje, že informace nesmí být v rozporu s obsahem návrhu smlouvy, který není dodavatel oprávněn měnit; viz zejména čl. X odst. 3 až 9 návrhu smlouvy.)

Prohlašujeme, že nabízené licence Microfocus DataProtector jsou dle licenčního modelu firmy Microfocus dostačující pro provoz. Žádné přechodné období neplánujeme.

datadomain

White Paper

Data Domain Data Invulnerability Architecture

Ensuring Data Integrity and Recoverability

Abstract

No single mechanism is sufficient to ensure data integrity in a storage system. It is only through the cooperation of a multitude of mechanisms that establish successive lines of defense against all sources of errors that data recoverability can be assured.

Unlike traditional general purpose storage systems, Data Domain systems have been designed explicitly for data protection.

This paper focuses on four key elements of the Data Domain Data Invulnerability Architecture which, in combination, provide the industry's highest levels of data integrity and recoverability:

- End-to-end verification
- Fault avoidance and containment
- Continuous fault detection and healing
- File system recoverability

Storage System Data Integrity

Behind all their added value, specialized storage systems are built on software and general purpose computing components that can all fail. Some failures have an immediate visible impact such as the total failure of a disk drive. Other failures are subtle and hidden such as a software bug that causes latent file system corruption only discovered at read time.

To ensure data integrity in the face of such failures, the best storage systems include various data integrity checks, and are generally optimized for performance and system availability, not data invulnerability. In the final analysis, they assume that backups get done, and make design tradeoffs that favor speed over guaranteed data recoverability. For example, no widely used primary storage file system reads data back from disk to ensure it was stored correctly; to do so would compromise performance. But data can't be considered invulnerable if it isn't stored correctly in the first place.

In backup-to-disk, the priority must be data invulnerability over performance and even availability. Unless the focus is on data integrity, the backup data is at risk. If the backup data is at risk, then when the primary copy of the data is lost, recovery is at risk.

Most backup-to-disk storage systems are just primary storage systems built out of cheaper disks. As such, they inherit the design philosophy of their primary storage predecessors. Though labeled as backup-to-disk products, their designs emphasize performance at the expense of data invulnerability.

Data Domain Data Invulnerability Architecture

Data Domain deduplication storage systems represent a clean break from conventional storage system design thinking and introduce a radical premise: what if data integrity and recoverability was the most important goal? If one imagines a tapeless IT department, one would have to imagine extremely resilient and protective disk storage. Data Domain systems have been designed from the ground up to be the storage of last resort.

Because the Data Domain operating system (DD OS) is purpose-built for data protection, its design elements comprise an architectural design whose goal is data invulnerability. There are four critical areas of focus:

- End-to-end verification
- Fault avoidance and containment
- Continuous fault detection and healing
- File system recoverability

Even with this model, it is important to remember that DD OS is only as good as the data it receives. It can do an end-to-end test of the data it receives within its system boundaries, but it cannot know whether that data has been protected by all steps in the network on the way to it. If there is an error in the backup network that causes data corruption, or if the data is corrupted in place in primary storage, DD OS cannot repair it. It remains prudent to test recovery to the application level on a periodic basis.

End-to-End Verification

Since every component of a storage system can introduce errors, an end-to-end test is the simplest path to ensure data integrity. End-to-end verification means reading data after it is written and comparing it to what it is supposed to be, proving that it is reachable through the file system to disk, and proving the data is what it is supposed to be.

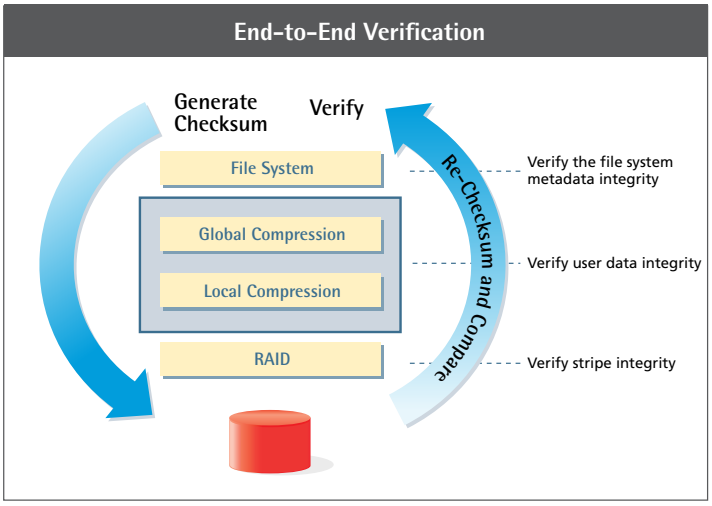


Figure 1. The end-to-end check verifies all file system data and metadata. As data comes in, a strong checksum is computed. The data is deduplicated and stored in the file system. After all data is flushed to disk, it is read back, re-checksummed and the checksums are compared to verify that both the data and the file system references to the data are stored correctly.

When DD OS receives a write request from backup software, it computes a huge checksum over the constituent data. After analyzing the data for redundancy, it stores the new data segments and all of the checksums.

After the I/O dust has settled on a backup and all the data has been synched to disk, DD OS verifies that it can read the entire file from the disk platter and through the Data Domain file system, and that the checksums of the data read back match the checksums of the written. This ensures that the data on the disks is readable and correct and that the file system metadata structures used to find the data are also readable and correct. The data is correct and recoverable from every level of the system.

If there are problems anywhere along the way, for example if a bit has flipped on a disk drive, it will be caught. For the most part it can be corrected through self-healing as described below in Fault

Detection and Healing. If for any reason it can't be corrected, it will be reported immediately, and a backup can be repeated while the data is still valid on the primary store.

Conventional, performance-optimized storage systems cannot afford such rigorous verifications. Backup-to-disk requires them. The tremendous data reduction achieved by Data Domain Global Compression™ reduces the amount of data that needs to be verified and makes such verifications possible.

Fault Avoidance and Containment

The next step in protecting the data is to make sure the data which was verified to be correct stays correct. Ironically, the biggest risk to file system integrity is file system software errors when writing new data. It is only new writes that can accidentally scribble on existing data, and new updates to file system metadata that can mangle existing structures.

Because the Data Domain file system was built to protect data as its primary goal, its design protects even against bugs in its own software that could put existing backups at risk. It accomplishes through a combination of design simplicity which reduces the chance of bugs in the first place and several fault containment features which make it difficult for the inevitable software bugs to corrupt existing data.

Data Domain systems are equipped with a specialized log-structured file system that has four important benefits.

New data never overwrites good data.

Unlike a traditional file system, which will often overwrite blocks when data changes using its old block address, DDFS only writes to new blocks. This isolates any incorrect overwrite (a software bug type of problem) to only the newest backup data. Older versions remain safe.

Fewer complex data structures.

In a traditional file system, there are many data structures (e.g. free block bit maps and reference counts) which support very fast block update. In a backup application, the workload is primarily sequential writes of new data. Because the application is simpler, fewer data structures are required to support it. As long as the system can keep track of the head of the log, new writes will touch old data. This design simplicity greatly reduces the chances of software errors that could lead to data corruption.

NVRAM for fast, safe restart.

The system includes a non-volatile RAM write buffer into which it puts all data not yet safely on disk. The file system leverages the security of this write buffer to implement a fast, safe restart capability. The file system includes many internal logic and data structure integrity checks. If any problem is found by one of these checks, the file system restarts itself afresh. The checks and restarts provide early detection and recovery from the kinds of bugs that can corrupt data. As it restarts, the Data Domain file system verifies the integrity of the data in the NVRAM buffer before applying it to the file system and so ensures that no data is lost due to the restart. Because the NVRAM is on separate device, it protects the data from bugs that can corrupt data in RAM. Because the RAM is non-volatile, it also protects against power failures. Though the NVRAM is important for ensuring the success of new backups, the file system guarantees the integrity of old backups even if the NVRAM itself fails.

No partial stripe writes.

Traditional primary storage disk arrays, whether RAID-1, RAID-4, RAID-3, RAID-5, or RAID-6, can lose old data if, during a write, there is a power failure which causes a disk to fail. This is because disk reconstruction depends on all the blocks in a RAID stripe being consistent but during a block write there is a transition window where the stripe is inconsistent, reconstruction of the stripe would fail, and the old data on the failed disk would be lost. Enterprise storage systems protect against this with NVRAM or uninterruptible power supplies. But, if these fail because of an extended power outage, the old data could be lost and a recovery attempt could fail. For this reason, Data Domain systems never update just one block in a stripe. Following the no-overwrite policy, all new writes go to new RAID stripes and those new RAID stripes are written in their entirety[1]. The verification after write ensures that the new stripe is consistent. New writes don't put existing backups at risk.

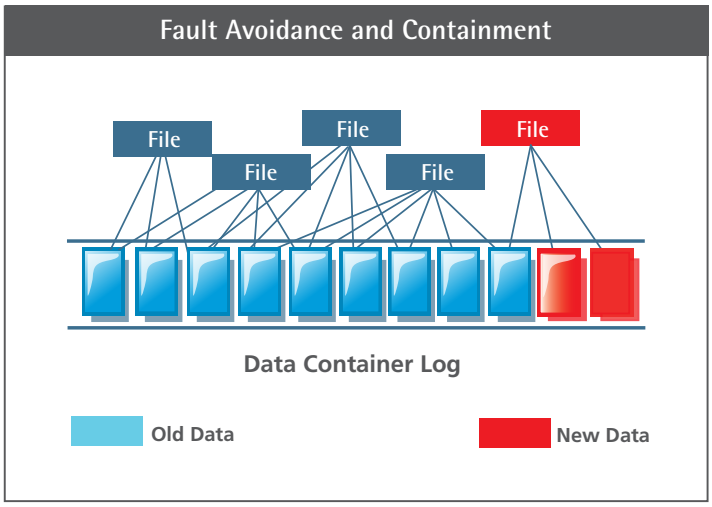


Figure 2: New data never puts old data at risk. The data container log never overwrites or updates existing data. New data is always written in new containers (in red). The old containers and references remain in place and are safe even in the face of software bugs or hardware faultsthat may occur when storing new backups.

Data Domain systems are designed to minimize the number of standard storage system errors. If more challenging faults happen, it takes less time to find them, corrent them, and notify the operator.

[1] The gateway product, which relies on external RAID, is unable to guarantee that there are no partial stripe writes.

Continuous Fault Detection and Healing

No matter the software safeguards in place, it is the nature of computing hardware to have occasional faults. Most visibly in a storage system, disk drives can fail. But, other more localized or transient faults also occur. An individual disk block may be unreadable or there could be a bit flip on the storage interconnect or internal system bus. For this reason, DD OS builds in extra levels of data protection to detect faults and recover from them on-the-fly and so ensure successful data restore operations.

RAID-6: Double disk failure protection, read error correction.

RAID-6 is the foundation for Data Domain's continuous fault detection and healing. Its powerful dual-parity architecture offers significant advantages over conventional architectures including RAID-1 (mirroring), RAID-3, RAID-4 or RAID-5 single-parity approaches.

RAID-6:

- protects against two disk failures,
- protects against disk read errors during reconstruction,
- protects against the operator pulling the wrong disk,
- guarantees RAID stripe consistency even during power failure without reliance on NVRAM or UPS and
- verifies data integrity and stripe coherency after writes.

By comparison, once a single disk is down in these other RAID approaches, any further simultaneous disk error will cause data loss. A system whose focus is data protection must include the extra level of protection RAID-6 provides.

On-the-fly error detection and correction.

To ensure that all data returned to the user during a restore is correct, the Data Domain file system stores all of its on-disk data structures in formatted data blocks. These are self-identifying and covered by a strong checksum. On every read from disk, the system first verifies that the block read from disk is the block expected. It then uses the checksum to verify the integrity of the data. If any issue is found, it asks RAID-6 to use its extra level of redundancy to correct the data error. Because the RAID stripes are never partially updated, their consistency is ensured and thus so is the ability to heal an error when it is discovered.

Scrub to ensure data doesn't go bad.

On-the-fly error detection works well for data that is being read, but it does not address issues with data that may be unread for weeks or months before it is needed for a recovery. For this reason, Data Domain systems actively re-verify the integrity of all data every week in an ongoing background process. This scrub process will find and repair grown defects on the disk before they can become a problem.

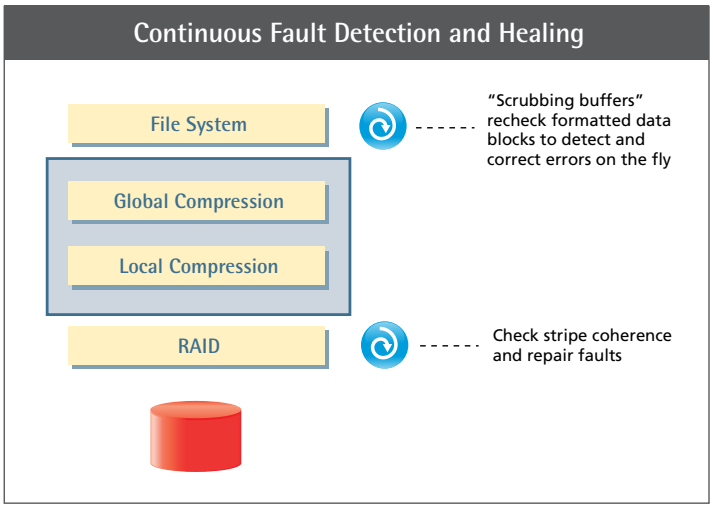


Figure 3: Continuous fault detection and healing protects against storage system faults. The system periodically rechecks the integrity of the RAID stripes and the container log and uses the redundancy of the RAID system to heal any faults. During every read data integrity is reverified and any errors are healed on the fly.

Through RAID-6, on-the-fly error detection and correction, and ongoing data scrubbing, most computing-system and disk drive-generated faults can be isolated and overcome with no impact on system operation or data risk.

File System Recoverability

Though every effort is made to ensure there are no file system issues, the Data Invulnerability Architecture anticipates that, being man-made, some system some time may have a problem. It therefore includes features to reconstruct lost or corrupted file system metadata and also file system check tools that can bring an ailing system safely back on line quickly.

Self-describing data format to ensure metadata recoverability.

Metadata structures, such as indices which accelerate access, are rebuildable from the data on disk. All data is stored along with metadata which describes it. If a metadata structure is somehow corrupted, there are two levels of recoverability. First, a snapshot is kept of the file system metadata every several hours; recoverability can rely on this point in time copy. Second, the data can be scanned on disk and the metadata structure can be rebuilt. These capabilities enable recoverability even if there is a worst-case corruption of the file system or its metadata.

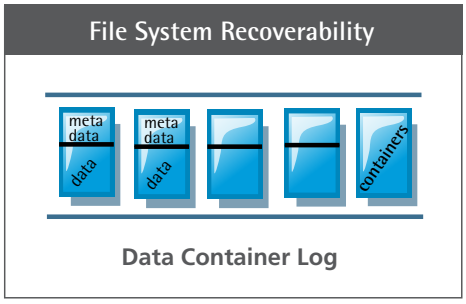


Figure 4. Data is written in a self-describing format. If necessary the file system can be recreated by scanning the log and rebuilding it from the metadata stored with the data.

FS check, if needed, is fast.
In a traditional filesystem, consistency is not checked on line at all. Data Domain systems check through initial verification at after each backup to ensure consistency for all new writes. The usable size of a traditional file system is often limited by the time it would take to recover the file system in the event of some sort of corruption. Imagine running fsck on traditional file system with more than 80 TB of data. The reason the checking process can take so long is that the file system needs to sort out where the free blocks are so that new writes don't end up overwriting existing data accidentally. Typically this entails checking all references to rebuild free block maps and reference counts. The more data in the system, the longer this takes. In contrast, since the Data Domain file system never overwrites old data and doesn't have block maps and reference counts to rebuild, it only has to verify where the head of the log is to safely bring the system back online to restore critical data.

Conclusion

No single mechanism is sufficient to ensure data integrity in a storage system. It is only through the cooperation of a multitude of mechanisms that establish successive lines of defense against all sources of errors that data recoverability can be assured.

Unlike a traditional storage system that has been repurposed from primary storage to data protection, Data Domain systems have been designed from the ground up explicitly for data protection. The innovative Data Invulnerability Architecture lays out the industry's best defense against data integrity issues. Advanced verification ensures that new backups are stored correctly. The no-overwrite, log-structured architecture of the Data Domain file system together with the insistence on full-stripe writes ensures that old backups are always safe even in the face of software errors during new backups. Meanwhile, the simplicity and robust implementation reduce the chance of software errors in the first place.

The above mechanisms protect against problems during the storage of backups, but faults in the storage itself also threaten data recoverability. For this reason, the Data Invulnerability Architecture includes a proprietary implementation of RAID-6 which protects against up to two disks failures, can rebuild a failed disk even if there is a data read error, and corrects errors on-the-fly during read. It also includes a continuous scrub process that actively seeks out and repairs latent faults before they become a problem.

The final line of defense is the recoverability features of the Data Domain file system. The self-describing data format enables the reconstruction of file data even if various metadata structures are corrupted or lost. And, the fast file system check and repair means that even a system holding dozens of terabytes of data won't be offline for long if there is some kind of problem.

Data Domain
2421 Mission College Blvd.
Santa Clara, CA 95054
866-WE-DDUPE; 408-980-4800
sales@datadomain.com
22 international offices: datadomain.com/company/contacts.html

WP-DIA-0308

WHITEPAPER

DELL EMC DATA DOMAIN RETENTION LOCK SOFTWARE

A Detailed Review

ABSTRACT

Enterprises continue to see an exponential growth in the structured and unstructured data that is proliferating across their primary storage systems. Customers realize that the majority of this data is seldom accessed; yet they cannot delete this data given the compliance retention requirements for business records. As organizations drive formal adoption of archiving, IT administrators need cost-effective ways for their fast-growing archive storage needs, including compliance retention. This white paper introduces the Dell EMC Data Domain Retention Lock software that provides immutable file locking and data retention capabilities to meet a broad class of corporate governance and regulatory compliance (SEC 17a-4(f)) standards of archive data stored on Data Domain systems.

August, 2017

Table of Contents

EXECUTIVE SUMMARY

Across the industry, enterprises continue to see an exponential growth in the structured and unstructured data that is proliferating across their primary storage systems. Customers realize that the majority of this data (as it ages with time) is not accessed often, yet they cannot delete this data because corporate governance and regulatory compliance (SEC17a-4(f)) standards mandate that data for business records must be securely retained for long periods of time (see Figure 1). As a result, companies are rapidly adopting formal archiving processes – so much so that the disk-based archiving market is forecasted to grow at a ~35% CAGR1 from 2010 through 2015.

Figure 1: Archive applications apply secure retention attributes

Almost all of enterprise data ranging from applications for processing content such as HR records or insurance document to traditional file/email records fall under strict retention guidelines. In addition, compliance retention policies continue to expand to include a broader variety of structured and unstructured data types. For optimal storage efficiency and data protection, customers require an archive storage system with:

- Support for both governance and compliance archive data with multiple retention periods on a single system
- Support for the majority of regulatory compliance standards including Security and Exchange Commission (SEC), Sarbanes-Oxley (SOX), Commodity Futures Trading Commission (CFTC), Food and Drug Administration (FDA), etc.
- Support for industry standard protocols (such as CIFS, NFS) for seamless integration with leading archive applications across various archive segments of file archive, email archive, enterprise content management (ECM) archive, database archive, etc.
- Next-generation protection storage that
    - Reduces the archive storage requirement with native compression and inline deduplication technology
    - Preserves all the data on the platform built of “storage of last resort” with the Data Domain Data Invulnerability Architecture
    - Enables consolidation of backup and archive data on a single system
    - Enables offsite protection via network-efficient replication

Dell EMC Data Domain Retention Lock® (DD Retention Lock) software provides immutable file locking and secure data retention capabilities for customers to meet both corporate governance and regulatory compliance standards, such as SEC 17a-4(f). DD Retention Lock provides the capability for IT administrators to apply retention policies at an individual file level. This software enables customers to leverage their existing Data Domain appliances to consolidate backup and archive data in accordance with governance and regulatory compliance standards.

[1] *IDC Report #230762, Archive Disk Based Storage Market: IDC WW Archival Storage Solutions 2010 – 2015 Forecast.*

AUDIENCE

This white paper is intended for Dell EMC customers, system engineers, partners, and members of the Dell EMC and partner professional services community who are interested in learning more about the DD Retention Lock software option.

INTRODUCTION

Data Domain Retention Lock software provides immutable file locking and secure data retention capabilities to meet a broad class of corporate governance and regulatory compliance (SEC 17a-4(f)) standards for archive data stored on Data Domain systems. This whitepaper explains the inner workings of both the Data Domain Retention Lock Governance edition and Data Domain Retention Lock Compliance edition.

This white paper will illustrate, how this software can be used to:

- Co-locate both governance and compliance data having different retention periods on the same Data Domain system
- Seamlessly integrate with your existing or new archiving application infrastructure to efficiently archive file/email, enterprise content management (ECM), database data and more
- Extend the use of your Data Domain system to consolidate archive data with backup data to maximize storage efficiency

This paper describes customer use cases, gives a product overview, and covers the interaction with other enterprise features such as replication. The security enhancements made specifically for the DD Retention Lock Compliance further allows deployment of strict compliant archive data along with governance archive and backup data on the same Data Domain system.

SECURE RETENTION OF ARCHIVE DATA

Unlike backup data, which is a secondary copy of data for recovery purposes, archive data is a primary copy of the data retained for long-term retention, secure and compliance retention purposes. As data ages and is seldom accessed, this data should be moved to archive storage, where it can still be accessed, but no longer occupies valuable primary storage space.

Archive data is usually stored for long-term with compliance retention policies and occasionally retrieved for eDiscovery needs. Since archive data is the primary copy of a data, IT administrators must ensure that the integrity of the data meets corporate governance rules and regulatory compliance (e.g. SEC 17a-4(f), etc.) standards.

GOVERNANCE ARCHIVE DATA REQUIREMENTS

Corporate governance standards for secure archive data retention are generally considered to be lenient in nature – allowing for flexible control of retention policies but not at the expense of integrity of the data during the retention period. These standards apply to environments where the system administrator is trusted with his or her administrative actions. The storage system has to securely retain archive data per corporate governance standards and needs to meet the following set of requirements:

- Allow archive files to be committed for a specific period of time during which the contents of the secured file cannot be deleted or modified
- Allow for deletion of the retained data once the retention period expires
- Allow for seamless integration with existing archiving application infrastructure through industry standard protocols such as CIFS and NFS
- Provide flexible retention policies such as allow extending the retention period of an archived file, revert of locked state of the archived file, etc.

- Ability to replicate both the retained archive files and retention period attribute to a destination site to meet the disaster recovery (DR) needs for archive data

COMPLIANCE ARCHIVE DATA REQUIREMENTS

The records retention requirements stipulated by the Securities & Exchange Commission ("SEC") Rule 17a-4(f) that defines compliance standards for archive storage expressly allows records to be retained on electronic storage media, subject to meeting certain conditions. Specifically, the conditions and requirements that an archive storage system must meet to be SEC compliant are:

- Preserve the records exclusively in a non-rewritable, non-erasable format. Specifically, as defined in the Rule itself, this requirement "is designed to ensure that electronic records are capable of being accurately reproduced for later reference by maintaining the records in unalterable form."
- Verify automatically the quality and accuracy of the storage media recording process
- Serialize the original, and if applicable, duplicate units of storage media, and the time-date for the required retention period for information placed on such electronic storage media
- Store separately from the original a duplicate copy of the record stored on any medium acceptable under 240.17a-4 for the time required

DD Retention Lock Compliance edition when deployed on the Dell EMC Data Domain storage system meets all of the above-mentioned SEC requirements set forth in Rule 17a-4(f), which expressly allows archive data to be retained on electronic storage media and meet strictest compliance requirements.

TYPICAL DEPLOYMENT ENVIRONMENTS

Enterprises have a slew of applications ranging from email servers to rich content management applications – and, the data across these application environments need to either meet governance or compliance retention. Below are some typical deployment environments:

- Archiving environments that are enforced for secure data retention requirements in line with corporate governance standards on existing or new archive data
- Archiving environments, specifically in industry verticals such as financial services, finance and banking, healthcare and pharmaceutical firms, legal and law firms that need to retain enterprise data in accordance with the strict retention requirements set forth by regulatory compliance standards (SEC 17a-4(f), etc.)
- Backup environments that are looking to store and securely retain archive data on the same deduplication based storage to drive further storage efficiency across the complementary workloads of backup and archive
- Environments where a net new end-to-end archiving solution is being architected and is required to seamlessly integrate with leading archive applications – such as Dell EMC SourceOne or Veritas Enterprise Vault
- Environments that want to reduce the primary storage footprint and spend by archiving inactive and aged data from primary storage system

DATA DOMAIN RETENTION LOCK SOFTWARE OVERVIEW

Dell EMC Data Domain Retention Lock software allows storage administrators, storage administrators, and compliance officers to meet data retention requirements for archive data when stored on a Data Domain system. DD Retention Lock software prevents files from being modified or deleted for a user-defined retention period.

Once the retention period expires, files can be deleted by the application, but cannot be modified. Files that are written to a Data Domain system but are not committed to be retained can be modified or deleted at any time. DD Retention Lock software comes in two editions – Dell EMC Data Domain Retention Lock Governance edition and Dell EMC Data Domain Retention Lock Compliance edition (see Figure 2).

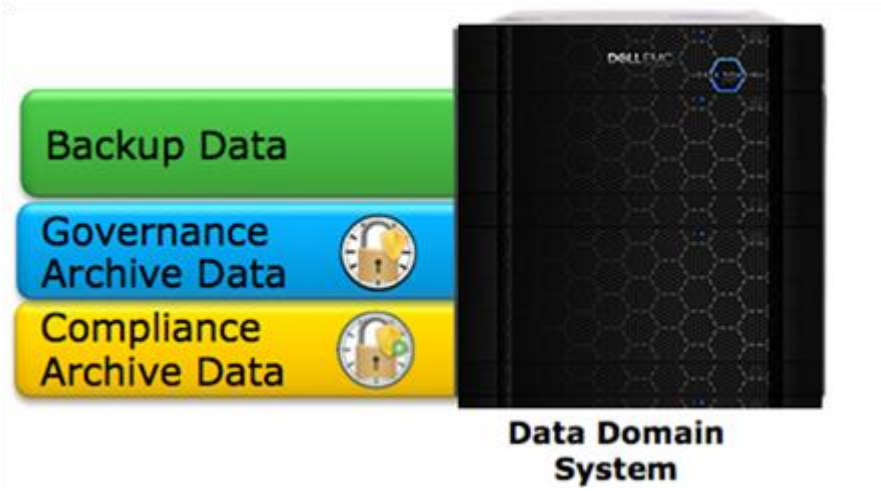


Figure 2: DD Retention Lock Governance edition and DD Retention Lock Compliance edition can *coexist* on the same Data Domain system.

- DD Retention Lock Governance edition maintains the integrity of the archive data with the assumption that the system administrator is generally trusted and thus any actions taken by the system administrator are valid to maintain the integrity of the archive data.
- DD Retention Lock Compliance edition is designed to meet strict regulatory compliance standards such as those of Security and Exchange Commission for 17a-4 Records (SEC 17a-4(f)).

CONSOLIDATE GOVERNANCE AND COMPLIANCE ARCHIVE DATA

Customers are looking for a storage solution that can consolidate both governance archive and compliance archive data on a single storage system. They want the storage system to be very easy to configure with granular management with built-in protection to help prevent common administrators mistakes.

To facilitate this consolidation of varied archive retention needs, a Data Domain Managed Tree (MTree) is used. MTree(s) are user-defined logical partitions of the Data Domain file system that enable granular management of data stored on a Data Domain system. Customers can enable DD Retention Lock software at an individual MTree level. A Data Domain system with DD Retention Lock Compliance can be configured to have one or more MTree(s) as compliance MTree(s) and/or with DD Retention Lock Governance can be configured to have one or more MTree(s) as governance MTree(s) (see Figure 3).

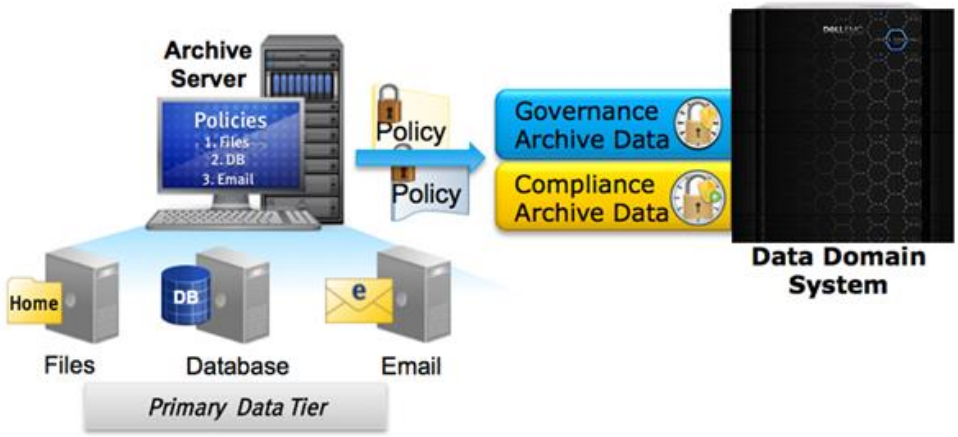


Figure 3: Data Domain Retention Lock software allows customers to apply different retention policies specific to the archive data type such as files, emails, database records, ECM data, etc.

This enables customers to be able to deploy both DD Retention Lock editions on the same Data Domain system[2].

This flexible deployment model allows customers to apply different retention periods for different types of archive data stored on MTrees (i.e. file, email, ECM, database archive, etc.) and meet both corporate governance and regulatory compliance standards on the same Data Domain system.

Customers must enable DD Retention Lock at an individual MTree level before any archive data stored on that MTree can be locked for governance or compliance retention. Before an MTree can be enabled with DD Retention Lock Compliance edition, the Data Domain system has to be configured for additional security measures (outline below). These measures ensure that administrative actions that could compromise the integrity of records are not under the control of just one administrative person. For specific instructions on configuring and enabling DD Retention Lock software, please refer to the *Dell EMC Data Domain Operating System Admin Guide*.

FILE LOCKING PROTOCOL

Once an archive file has been migrated onto a Data Domain system, it is the responsibility of the archiving application (or, manual scripts) to set and communicate the retention period attribute of the archive file to the Data Domain system. The archiving application sends the retention period attribute over standard industry protocols (CIFS, NFS), then the Data Domain system will enforce that retention period with DD Retention Lock.

The retention period attribute used by the archiving application is the last access time: the “atime”. DD Retention Lock software allows granular management of retention periods on a file-by-file basis. As part of the configuration and administrative setup process of the DD Retention Lock software, a minimum and maximum time-based retention period for each MTree (Managed Tree) is established. This ensures that the (atime) retention expiration date for an archive file is not set below the minimum or above the maximum retention period.

Let’s consider an example – an archiving application stores an archive file on the Data Domain system and sets the last access time (atime) of the file to the desired retention time, that is, a point in time in the *future* at which the file may be deleted. The retention period (atime) specified for a file in the MTree must be *equal to or greater than* the minimum retention period and equal to or less than the maximum retention period for that MTree.

If the retention period from the archiving application is:

- Less than the current date/time, or
- Less than the minimum retention period per MTree, or
- Greater than the maximum retention period per MTree

Then an error condition (permission denied error, referred to as EACCESS – a standard POSIX error) will be returned to the archiving application thus providing additional protection. The only exception here is in the scenario where the retention period is less than the current time plus 12 hours (tolerance window), and then the atime update will be ignored without an error and the file will not be locked for secure retention on the Data Domain system.

The archiving application must set the atime value and DD Retention Lock must enforce it to avoid any modification or deletion of files under retention of the file on the Data Domain system. For example, Veritas Enterprise Vault (EV), a file/email/SharePoint archive application, archives records for a user-specified amount of time. When EV retention is in effect, these documents cannot be modified or deleted on the Data Domain system. When that time *expires*, Enterprise Vault can be set to automatically dispose of those records.

For specific best practices to securely retain archive data via Veritas Enterprise Vault on the Dell EMC Data Domain system please refer to *Dell EMC Data Domain and Veritas Enterprise Vault Integration Guide*. For Dell EMC SourceOne, please refer to *Dell EMC Data Domain* and *Dell EMC SourceOne Integration Guide*.

[2] Note, that a single MTree cannot be configured as both governance and compliance at the same time.

DATA DOMAIN RETENTION LOCK GOVERNANCE EDITION

DD Retention Lock Governance edition allows customers to maintain the integrity of the archive data with the assumption that the system administrator is generally trusted with all legal actions performed on the Data Domain system (see Figure 4).

By enabling DD Retention Lock Governance edition on an MTree, IT administrators can:

- Apply retention policies at an individual file level of the data set on the Governance enabled MTree for a specific period of time
- Delete an archive file via an archiving application after the retention period expires
- Update the default values of minimum and maximum retention periods per MTree
- Extend the retention time of locked archive files

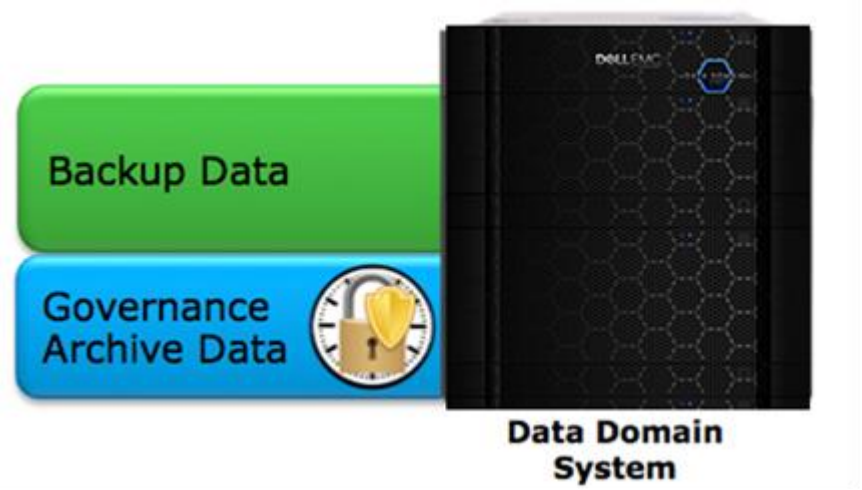


Figure 4: A Data Domain system can retain both Backup and Archive data that has to be retained per the corporate governance policies.

Locked files *cannot* be modified on the Data Domain system *even after* the retention period for the file expires. Archive data that is retained on the Data Domain system is **not** deleted automatically when the retention period expires; an archiving application must delete the file.

With DD Retention Lock Governance edition, IT administrators can meet secure data retention requirements while keeping the ability to update the retention period should the corporate governance policies change.

For example, an IT Administrator might want to:

- Revert the locked state of a file on a specified path name inside of an MTree
- Delete an MTree enabled with DD Retention Lock Governance

SYSTEM MANAGEMENT

Data Domain has designed an easy to use GUI in the Dell EMC Data Domain System Manager to help administrators monitor archived data. Alternatively, administrators can use available system commands (CLI).

Using the DD System Manager, customers can install the DD Retention Lock Governance license on the Data Domain system and can then enable DD Retention Lock Governance. DD System Manager provides the capability to update and modify the minimum and maximum retention period for MTrees. The DD System Manager GUI displays the various

states of the specific retention locked fields on the Data Domain system such as Unique Identification Number (UUID), etc. (see Figure 5 below)

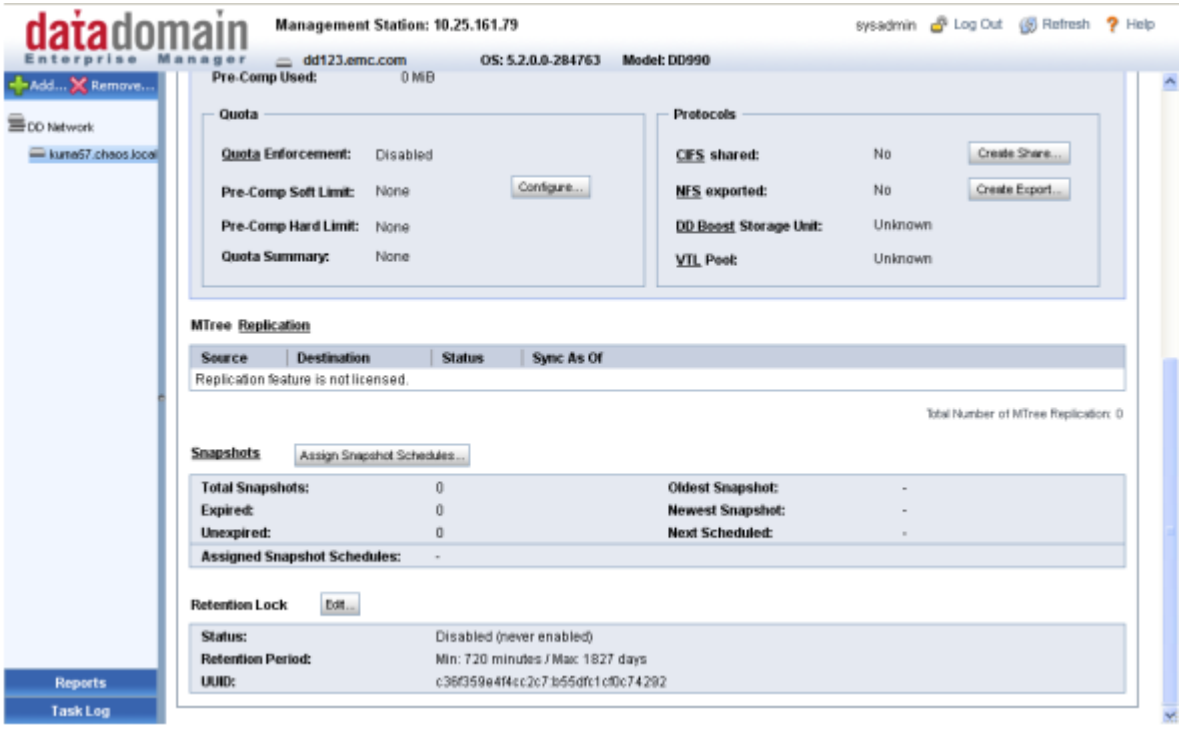


Figure 5: Data Domain System Manager showing Retention Period and UUID stat.

Please refer to the *Dell EMC Data Domain Operating System Admin Guide* and *Dell EMC Data Domain Operating System Command Reference Guide* for a detailed list and instructions on the full set of capabilities that are available for DD Retention Lock Governance edition on a Data Domain system.

DATA DOMAIN RETENTION LOCK COMPLIANCE EDITION

The DD Retention Lock Compliance edition meets the strict retention requirements of regulatory standards for electronic records such as SEC 17a-4(f) and other compliance standards that are practiced worldwide across industry verticals.

DD Retention Lock Compliance, when enabled on an MTree, ensures that all the files locked by an archiving application, for a time-based retention period cannot be deleted or overwritten under any circumstances until the retention period expires (see Figure 6). This is achieved via multiple hardening procedures such as:

- Requiring “dual” sign-on for certain administrative actions
- Completely disallowing operations that could compromise the state of locked and retained archive data
- Securing the system clock from illegal updates
- Audit logging for any operations that are executed upon the locked archive data
- Litigation hold allowing extension of the retention time of locked archive files
- Disabling various “doors” of access where someone could compromise the state of the locked data or the state of the retention attributes

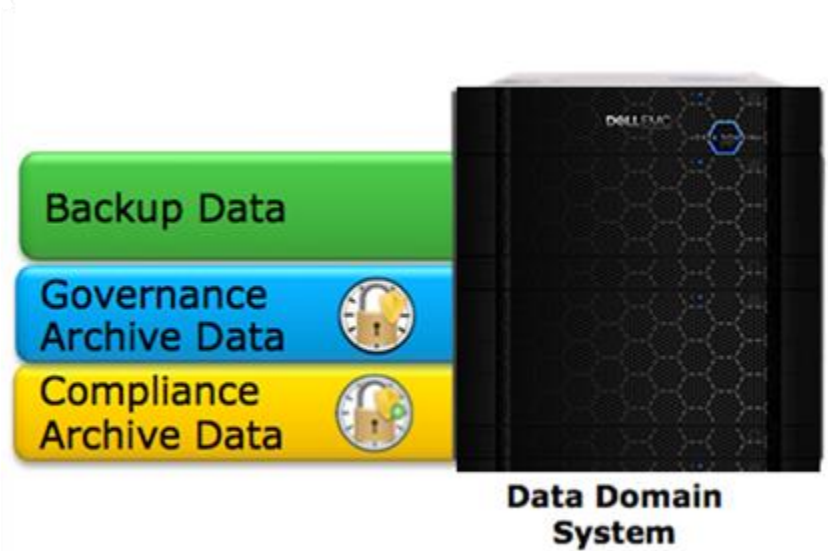


Figure 6: A Data Domain system that is being used for backup and governance archive data can be configured for the additional use case of archive data that needs to meet regulatory compliance (SEC 17a-4f) requirements.

"DUAL" SIGN-ON REQUIREMENTS

The most stringent requirement from compliance standards (such as SEC 17a-4(f)) is to ensure that any actions that could compromise the integrity of archive files prior to expiration of the retention period can only be executed by deliberate physical destruction methods.

To meet this requirement, DD Retention Lock Compliance edition provides a "dual" sign-on capability. This requires sign-on by the regular system administrator plus sign-on by a second authorized person (also referred to as "Security Officer") to perform certain administrative actions (see Figure 7). This ensures certain administrative actions are under the purview and control of higher authority above and beyond the system administrator.

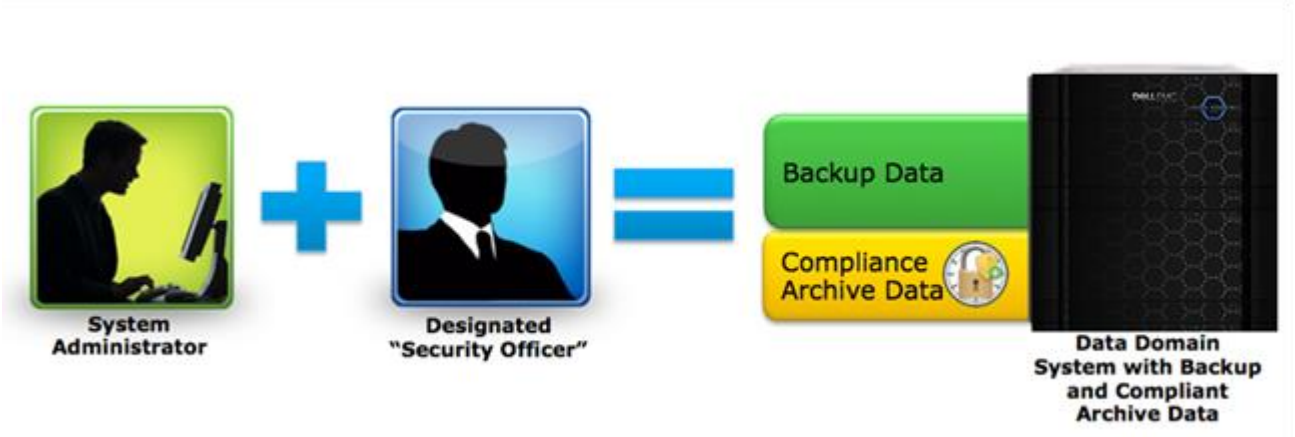


Figure 7: "Dual" sign-on capability of DD Retention Lock Compliance edition ensures that compliant archive data cannot be deleted under any circumstances.

It is possible to have *multiple* Security Officers configured on a single Data Domain system. Thereby, any one of the Security Officers can authorize system commands on the Data Domain system that require Security Officer credentials. It is important to note that the system administrator creates the first Security Officer; and after that only that designated Security Officer can add more Security Officers as authorized users on the Data Domain system. Having multiple

Security Officers is important for scenarios when one or more Security Officer is not available and certain critical operations have to be performed. In addition, creating multiple Security Officers in a single Data Domain system can prevent misuse of Security Officer authorization. Please refer to *Technical Assessment and Report from Cohasset Associates*, industry leading records management firm, on Security Officer model of DD Retention Lock Compliance edition.

Specifically, the primary administrative actions that require a dual sign-on are:

- Extending minimum or maximum retention periods of the MTree
- Renaming the MTree
- Deleting the installed DD Retention Lock Compliance license from the Data Domain system
- Other system support or maintenance actions that could potentially compromise the integrity of stored record files where the retention period has not expired

Additionally, the following are the operations or system commands that are completely locked down and therefore **cannot** be executed by anyone on the Data Domain system that has a DD Retention Lock Compliance installed and enabled:

- Destroying the entire Data Domain file system
- Deleting an MTree with DD Retention Lock Compliance enabled – even if the MTree is empty and has no locked files stored on it
- Disabling DD Retention Lock Compliance on an MTree after it's been enabled
- Reverting the retention state of the locked files on an MTree with DD Retention Lock Compliance enabled

SECURE SYSTEM CLOCK

Time-based retention is one of the primary requirements of regulatory compliance standards. In order to meet this requirement, a Data Domain system needs to ensure that any undesired changes to the system clock cannot be executed. Specifically, DD Retention Lock Compliance prevents users from changing the system clock via either system commands (CLIs) or by using the DD System Manager.

To ensure that the system clock cannot be modified, DD Retention Lock Compliance:

- Requires Security Officer approval for any system commands that could change the system clock
- Makes the system clock value persistent in the underlying storage by periodically writing it in the metadata file on the system
    - Then it will continuously check the current system clock time against this persistent system clock value
    - If the current time on the system clock is not within "acceptable" bounds (15 minutes) from this persistent time information, then this is considered as a *skew*
    - DD Retention Lock Compliance keeps track of the total skew for the current year and if the total skew becomes more than 2 weeks in that year, the system is locked down and the Data Domain file system will shut down
    - If the Data Domain system is locked down due to security clock violation, then it can only be resumed by providing Security Officer credentials

AUDIT LOGGING

Auditing capabilities are a requirement to meet compliance standards. Specifically, audit logs have to be kept for operations on locked data. This puts a requirement both on the archiving application and the Data Domain system. The logging of operations on the customer data is maintained by the archive application being used. Separately, the Data Domain system logs all management operations that affect locked files stored on the Data Domain system. All relevant operations are logged in a separate audit log that is available to the Security Officer. The system administrator cannot modify the audit log file on the Data Domain system that has DD Retention Lock Compliance edition installed and enabled.

LITIGATION HOLD

During periods of legal discovery, enterprises may be required by law to maintain their compliance data for extended periods of time. Dell EMC Data Domain systems provide this capability via litigation hold that allows the administrator to extend the retention lock periods on a per file basis beyond the maximum retention period of the containing MTree. Such an extension is allowed to a maximum period of 70 years from the current time. This capability can be driven via Archiving applications that support such extension capabilities.

REGULATORY COMPLIANCE STANDARDS

Compliance standards exist to verify that products comply with different regulatory standards across industry verticals. It's critical that customers ensure that a product used for secure retention of archive data receive a technical certification of standards compliance from a 3rd party with deep knowledge of regulatory standards and industry credibility.

In general, there are five United States federal regulations; the most notable being SEC Rule 17a-4(f). There is one international ISO standard and one European Union electronic records management guidance document. Refer to Table 1 below that lists various compliance regulations, industries impacted and the relevant DD Retention Lock edition that meets those requirements:

Compliance Regulation	Regulatory Agency	Industry/Vertical Impacted	Data Domain Retention Lock software
Sarbanes-Oxley (SOX)	Securities & Exchange Commission (SEC)	Public Companies	DD Retention Lock Compliance edition
SEC 17a-4(f)	Securities & Exchange Commission (SEC)	Financial Services	DD Retention Lock Compliance edition
21 CFR Part 11	Food and Drug Administration (FDA)	Pharmaceutical	DD Retention Lock software
CFTC Rule 1.31b	Commodity Futures Trading Commission	Financial Services	DD Retention Lock Compliance edition
HIPAA	US Health and Human Services	Healthcare Services	DD Retention Lock software
ISO Standard 15489-1	International Standards Organization	Public Companies	DD Retention Lock Compliance edition
MoREQ 2 (Model Requirements for the Management of Electronic Records)	European Commission	Public Companies	DD Retention Lock Compliance edition

Table 1: Summary of Regulatory Standards that DD Retention Lock software meets - from a Compliance Storage requirements perspective

TECHNICAL ASSESSMENT

Dell EMC engaged Cohasset Associates, an industry-leading records management consulting firm, for a independent and thorough technical assessment of the capabilities of the DD Retention Lock Compliance edition relative to meeting the strict requirements set forth in SEC Rule 17a-4(f) and a number of other regulatory compliance standards practiced worldwide as highlighted in Table 1 above.

Cohasset Associates performed an extensive technical due diligence on the features and functionality that are available via the DD Retention Lock Compliance software and certified that the Dell EMC Data Domain Retention Lock Compliance on the Data Domain system meets the relevant requirements of SEC 17a-4(f).

This means that during the SEC required retention period a Data Domain system with DD Retention Lock Compliance software:

- Provides the integrated control codes and record file management capabilities that ensures protection of record files from overwrite or erasure
- Provides for initial and ongoing accuracy and quality of the stored records
- Uniquely identifies each record file and duplicate copy
- Provides for a duplicate copy of the record files and recovery from the duplicate copy if required

In summary, the DD Retention Lock Compliance edition enables Data Domain systems to be the:

- Industry's *first* inline deduplication storage system that provides immutable file locking and secure data retention capabilities that meet a broad class of industry's strictest compliance standards for archive data
- Industry's *first* inline deduplication storage system enabling customers to deploy and co-locate both backup and archive data that has to meet compliance retention requirements

SUPPORTED PROTOCOLS

DD Retention Lock software is qualified and certified with industry leading archiving applications such as Dell EMC SourceOne, Dell EMC DiskXTender, Veritas Enterprise Vault (EV), etc. and is compatible via the industry-standard, NAS-based (CIFS, NFS) Write-Once-Read-Many (WORM) protocols. For a complete list of archiving and tiering applications that are qualified on Data Domain systems, please refer to the *Data Domain Archiving Applications Compatibility Matrix*.

Customers using backup applications such as Dell EMC NetWorker and Veritas NetBackup, can also use custom scripts to control the DD Retention Lock software on the Dell EMC Data Domain systems. For information on creating custom scripts to manage the retention policies of individual files, please see the *Dell EMC Data Domain Operating System Admin Guide* and refer to the section on "DD Retention Lock".

Note a Data Domain system with the Data Domain Virtual Tape Library software only supports DD Retention Lock Governance edition. Additionally, please note the following considerations for this configuration:

- Virtual tapes are represented as files on the Data Domain file system
- When customer creates a storage pool (a collection of tapes that map to a directory on the file system)
- Once created, one can use DD Replicator and DD Retention Lock on this MTree

CONSIDERATIONS FOR REPLICATING ARCHIVE DATA

Many companies have minimized the use of tape automation in their IT infrastructure by deploying deduplication storage for backup and operational recovery – Dell EMC Data Domain deduplication storage systems have been the market leaders in this category. In general, operational recovery includes retention periods from a few weeks to a few months. In addition, Data Domain systems also continue to revolutionize for backup and archive data that needs to be retained for longer period of times (years). By consolidating backup and archive data on a Data Domain system, storage

requirements can be reduced in size by 10 to 30x, making disk cost-effective for onsite retention, and highly efficient for network-based replication to disaster recovery sites.

Like most storage platforms, configuring disaster recovery is critical to a Data Domain system deployment. It is important to keep a full replica of all stored data in a separate system in a remote site that is protected from disasters and catastrophes. For Data Domain systems, Dell EMC Data Domain Replicator software provides simple, fast, robust WAN-based disaster recovery for the enterprise. It offers numerous replication types and policies and also supports a wide variety of topologies to meet the needs of various deployments.

DD RETENTION LOCK GOVERNANCE AND REPLICATION

For archive data that is locked for a specified period of time on a Data Domain system, it is critical for customers to be able to maintain the replicated copy of both the locked data and the retention attributes on the destination Data Domain system for DR scenarios.

Collection replication, MTree replication, and directory replication replicate (see Figure 8 below) the locked or unlocked state of files that are stored on the Governance enabled MTrees (see Table 2 below). This ensures that files that are locked on the source system remain locked after replication to the destination system. Only the source Data Domain system needs a DD Retention Lock Governance license for the locked data to be replicated and stored in the locked state on the destination Data Domain system.

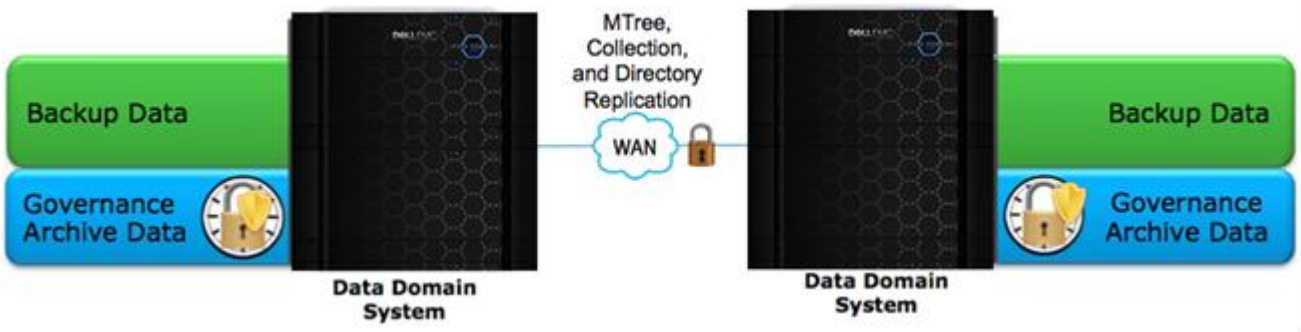


Figure 8: DD Replicator copies both the governance archive data under retention and associated retention periods from the source Data Domain system to the destination Data Domain system.

Replication Type	Support for replicating locked data	Replicate Min and Max Retenton Periods per MTree
Directory Replication	Yes	No
Collection Replication	Yes	Yes
MTree Replication	Yes	Yes

Table 2: Support for replicating locked data and metadata per Replication type

DD RETENTION LOCK COMPLIANCE AND REPLICATION

An absolute requirement for meeting compliance standards is to *"store separately from the original a duplicate copy of the record stored on any medium acceptable"*. Specifically, this rule from the SEC 17a-4(f) compliance standard requires that a separate copy of locked archive data must be stored on a secondary Data Domain system with the same retention attributes as the original. Therefore, DD Retention Lock Compliance must allow for replication of compliant archive data and make sure that both the source and destination systems meet compliance requirements (see Figure 9).

Figure 9: Either of MTree Replication or Collection Replication can be used to copy the backup and archive data from source Dell EMC Data Domain system to the destination Dell EMC Data Domain system

MTree replication or collection replication can be used to replicate the retention attributes of the locked archive files and associated MTrees to the destination Data Domain system. Here's an example scenario that expands on this capability for net new deployment of backup and archive (governance or compliance retention) data on a Dell EMC Data Domain system:

- Customer buys a pair of Data Domain systems and installs DD Replicator software, DD Retention Lock Governance software, and DD Retention Lock Compliance software.
- To consolidate both backup and archive data on the Data Domain system, the customer deploys backup data on MTree1, governance archive data on MTree2, and compliant archive data on MTree3.
- In this scenario, given that compliance archive data must be replicated to a destination Data Domain system, the customer uses MTree replication to meet disaster recovery requirements and consolidation needs of backup and archive data.

Furthermore, DD Retention Lock Compliance ensures that initialization, recover, and sync operations of collection replication will only proceed if the DD Retention Lock Compliance license is enabled on both the source and destination Data Domain systems. DD Retention Lock Compliance disallows replication from a compliant source Data Domain system to a destination Data Domain system that does not have DD Retention Lock Compliance enabled. Finally, DD Retention Lock Compliance ensures that any system commands or operations that either disable or break replication are under the purview of the Security Officer and can only be successfully executed after "dual" sign-on.

DD RETENTION LOCK AND DD EXTENDED RETENTION

DD Extended Retention software increases the storage scalability of a Data Domain system to enable cost-effective long-term retention of backup data on deduplicated disk. DD Retention Lock software is supported on DD systems that are enabled with DD Extended Retention software. Specifically, customers can install either DD Retention Lock Governance edition or DD Retention Lock Compliance edition or both on a Data Domain system with DD Extended Retention software.

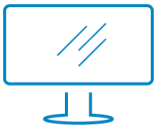
On a Data Domain system with DD Extended Retention software installed, files that are locked on the active tier, with either DD Retention Lock Governance edition or DD Retention Lock Compliance edition, will remain locked when migrated to the retention tier. Once the retention period expires, the files on the retention tier can be deleted, but cannot be modified, and the associated space can be reclaimed starting with DD OS 5.3 release.

CONCLUSION

Customers continue to see exponential growth in structured and unstructured data that is proliferating across their primary storage systems. While the majority of this data is seldom accessed, it cannot be deleted due to governance or compliance (SEC 17a-4(f)) retention requirements. This has resulted in rapid adoption of formal archiving processes and impressive growth in the disk-based archive storage market. Therefore, many customers are looking to invest in deduplication based storage platforms to consolidate complementary workloads of backup and archive (governance and/or compliance) data to reap additional cost savings and storage efficiency.

Dell EMC® Data Domain® deduplication storage systems continue to revolutionize disk backup, archiving, and disaster recovery with high-speed, inline deduplication. By consolidating backup and archive data on a Data Domain system, storage requirements can be reduced in size by 10 to 30x, making disk cost-effective for onsite retention, and highly efficient for network-based replication to disaster recovery sites. Additionally, the system is protected by the Dell EMC Data Domain Data Invulnerability Architecture providing the industry's best defense against data integrity issues.

By deploying Dell EMC Data Domain Retention Lock® software on Data Domain systems, customers can securely manage the governance or compliance retention requirements. Data Domain Retention Lock software provides immutable file locking for both governance and compliance archive data sets, seamlessly integrates with leading archiving applications, and allows the consolidation of both governance and compliance archive data with different retention periods on the same Data Domain system. The DD Retention Lock Compliance capability in the Dell EMC Data Domain Retention Lock software enables Data Domain systems to be the industry's first inline deduplication storage system that meets a broad class of industry's strictest compliance standards for archive data.



Learn more about Dell EMC Data Domain solutions

Contact a Dell EMC Expert

DELL Technologies

Data Sheet

DELL EMC POWERPROTECT DD SERIES APPLIANCES

Key benefits

Fast, secure, efficient data protection

- 1.5PB usable capacity in a single rack
- Up to 3PB capacity for long-term retention
- Improved logical capacity of typically 30% per TB*
- Instant access and instant restore of up to 64VMs and 100k IOPS*****
- High speed network connectivity – 10GbE, 25GbE and 100GbE
- Seamless integration and superior performance with PowerProtect Data Manager and Data Protection Suite
- Supports leading enterprise backup and archive applications

Industry-leading multi-cloud protection

- Software-defined protection storage on-premises and in-cloud with PowerProtect DD Virtual Edition (DDVE)
- DDVE scales up to 256TB in-cloud (AWS, Azure and Google Cloud)
- Improves in-cloud restore performance by up to 3x with single stream restores****
- Dell EMC Cloud Tier delivers simple and efficient long-term retention to a public, private or hybrid cloud
- Low-cost disaster recovery to the cloud

Operational simplicity

- Enhanced DD System Manager provides complete chassis view
- Lower administrative costs
- Single point of management for all DD series by PowerProtect DD Management Center

The ultimate protection storage appliance

DD series enables organizations to protect, manage and recover data at scale across their diverse environments. DD series is the next generation of Dell EMC Data Domain appliances, that are now setting the bar for data protection from edge to core to cloud. DD series provides the ecosystem support, efficiency, powerful data protection and cloud-enabled capabilities that customers have come to expect and appreciate from Data Domain and takes it to the next level.

The DD Operating System (DDOS) is the intelligence that powers DD series. It provides the agility, security and reliability that enables DD series to deliver high-speed, scalable and industry-leading multi-cloud protection storage for backup, archive and disaster recovery. DDOS integrates seamlessly with existing infrastructures, enabling ease-of-use with leading backup and archiving applications, and offers superior performance in conjunction with Dell EMC PowerProtect Data Manager and Data Protection Suite. When purchasing a new DD series appliance you can now consume DDOS as a subscription providing flexibility for deployment while minimizing up front costs.

Fast, secure and efficient data protection

DD series minimizes the risk of data loss and leverages the value of protected data, while meeting ever more demanding SLAs and increasing ROI. DDOS drives DD series to deliver up to 38% faster backups and up to 45% faster restores at higher compression levels.** This improved level of compression efficiency typically increases the logical capacity by 30% per TB*.

DD series can now scale up to a physical capacity of 1.5PB in a single rack, thereby utilizing minimal floor space and lowering power and cooling by up to 41%.*** By employing denser disk drives, DD series has lowered the required rack space by up to 39%.

DD series provides up to an additional 3PB of cloud capacity for long-term retention, with Dell EMC Cloud Tier.

DD series supports high availability within the single rack. By doing so, DD series can further reduce the total cost of ownership by reducing downtime in the unlikely event of a hardware failure. DD series delivers high speed networking connectivity with support for 25GbE and 100GbE network adapters.

* When compared to previous generation. Based on Dell EMC internal testing and field telemetry data. April 2021. Actual results may vary
** When compared to previous generation. Based on Dell EMC internal testing. April 2021. Actual results may vary.
*** When comparing 1 petabyte of data on a DD9800 with Cloud Tier and PowerProtect DD9900 with Cloud Tier. May 2021. Actual results may vary.
**** Based on Dell EMC internal testing comparing PowerProtect DD Virtual Edition in-cloud restore performance with DDOS 7.2 or later compared to DDOS 7.1. April 2021. Actual results may vary.
***** When using DDOS 7.7 and later on the DD9900. Based on Dell EMC internal testing. Actual results may vary. September 2021

Instant access and instant restore

Instant access and instant restore delivers high performance of VMs with up to 100K IOPS with the ability to instantly access up to 64 VMs simultaneously.*****

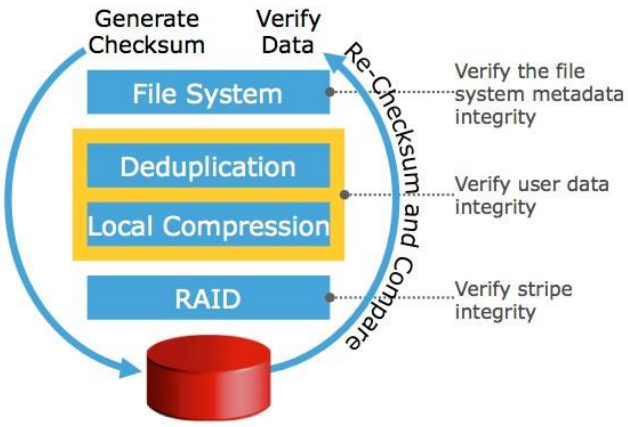
Instant access and instant recovery save time, minimizing mean time to repair (MTTR), by enabling instant access to data from the backup image on the included DD series SSD drives. It also saves primary storage space with the ability to manage data on the appliance itself and lowers cost by better utilizing the physical resources in both the data protection as well as the production environments.

In case of a failure or disaster recovery in a virtualized environment, DD series can spin-up production-oriented VMs immediately within the appliance itself. By doing so, the customer can continue their daily routine without experiencing any downtime, while the failed VMs are restored to the production environment.

Data Invulnerability Architecture

DD series is designed as the storage of last resort – providing you with the confidence that you can always reliably recover your data. The Data Invulnerability Architecture is built into DDOS and DD series to provide the industry's best defense against data loss. Inline write and read verification protects against and automatically recovers from data integrity issues during data ingest and retrieval while RAID-6 and hot spares protect against disk failure.

Capturing and correcting I/O errors inline during the backup process eliminates the need to repeat backup jobs, ensuring backups complete on time and satisfy service-level agreements. In addition, unlike other enterprise arrays or file systems, continuous fault detection and self-healing ensures data remains recoverable throughout its lifecycle on DD series.



End-to-end data verification

End-to-end data verification

End-to-end data verifications reads data after it is written and compares it to what was sent to disk, proving that it is reachable through the file system to disk and that the data is not corrupted. Specifically, when DDOS receives a write request from backup software, it computes a checksum over the data. After analysing the data for redundancy, it stores the new data segments and all the checksums. After all the data is written to disk, DDOS verifies that it can read the entire file from the disk platter and through PowerProtect DD, and that the checksums of the data read back match the checksums of the written data. This confirms the data is correct and recoverable from every level of the system.

Comprehensive DD series portfolio

	DDVE - 96TB	DD3300	DD6900	DD9400	DD9900
Backup Ingest (w/DD Boost)	Up to 11.2TB/hr	Up to 7.0TB/hr	Up to 33TB/hr	Up to 57TB/hr	Up to 94TB/hr
Logical Capacity (w/Active Tier)	Up to 4.8PB	Up to 1.6PB	Up to 18.7PB	Up to 49.9PB	Up to 97.5PB
Usable Capacity (w/Active Tier)	1TB-96TB	4TB-32TB	24TB-288TB	192TB-768TB	576TB-1.5PB

Logical capacity based on up to 50x deduplication (DD3300) and typically 65x deduplication (DD6900, DD9400, DD9900) based on additional hardware-assisted data compression of typically 30% better than previous generation. Actual capacity & throughput depends on application workload, deduplication, and other settings.

Seamless integration

DD series integrates easily with existing infrastructures, enabling ease-of-use with leading backup and archiving applications, and offers superior performance in conjunction with PowerProtect Data Manager and Data Protection Suite.

DD series can simultaneously support multiple access methods including NFS and/or CIFS, VTL, NDMP and DD Boost™ all applications and utilities can be supported in the same DD series at the same time to enable greater protection storage consolidation. A system can present itself as a file server, offering NFS, CIFS access over Ethernet; as a virtual tape library (VTL) over Fibre Channel; as an NDMP tape server over Ethernet; or as a disk target using application specific interfaces like DD Boost. DD VTL is qualified with leading open systems and IBMi enterprise backup applications.

Industry-leading multi-cloud protection

DD series simplifies and obtains operational efficiencies including resiliency and scale as you grow in any cloud environment – private, public and hybrid. DD series supports the most extensive cloud ecosystem – AWS, Azure, VMware Cloud, Google Cloud, Alibaba Cloud, and Dell EMC ECS to deliver excellent in-cloud data protection at reduced costs. DD series can natively tier deduplicated data to any supported cloud environment for long-term retention with Dell EMC Cloud Tier. DD series provides fast disaster recovery with orchestrated DR and provides an efficient architecture to extend on-premises data protection with lowered costs.

PowerProtect DD Virtual Edition

PowerProtect DD Virtual Edition (DDVE) leverages the power of DDOS to deliver software-defined protection storage on-premises and in-cloud. DDVE is fast and simple to download, deploy and configure - can be up and running in minutes. DDVE can be deployed on any standard hardware, converged or hyper-converged, and runs in VMware vSphere, Microsoft Hyper-V, KVM, as well as in-cloud with AWS, AWS GovCloud, VMware Cloud, Azure, Azure Government Cloud, and Google Cloud. DDVE is also certified with VxRail and Dell PowerEdge servers. An assessment tool can be run during deployment to check the underlying infrastructure and ensure it meets recommended requirements. A single DDVE instance can scale up to 256TB in-cloud (AWS, Azure and Google Cloud) and up to 96TB on-prem. Capacity can easily be moved between virtual systems and/or locations and can scale in increments of 1TB allowing you to grow capacity as the business demands. DDVE maintains the core DDOS features and includes DD Boost, DD Encryption and DD Replicator. DDVE can be configured and managed using DD System Manager and centrally manage multiple DDVE instances, on-premises and in-cloud, through PowerProtect DD Management Center.

Long-term retention and disaster recovery in-cloud

With Dell EMC Cloud Tier (Cloud Tier), DDOS can natively tier data to a public, private or hybrid cloud for long-term retention. Only unique data is sent directly from DD series to the cloud and data lands on the cloud object storage already deduplicated. It supports AWS, AWS Gov Cloud, Azure, Google Cloud, IBM Cloud, Alibaba Cloud, and Dell EMC Elastic Cloud Storage (ECS). With deduplication ratios of typically 65x, storage footprint is greatly reduced lowering overall TCO. With DDOS 7.7, Cloud Tier can scale up to 3PB of usable capacity. With DD Encryption, data in the cloud remains secure. Cloud Tier works with DDVE for on-prem deployments.

Dell EMC Cloud DR (Cloud DR) allows enterprises to copy backed-up VMs from their on-premises DD series environments to the public cloud (AWS, VMware Cloud on AWS, Azure) and to orchestrate DR testing and failover of workloads to the cloud in a disaster scenario with end to end orchestration.

Operational simplicity

DD series is very simple to install and manage resulting in lower administrative and operational costs. Administrators can access DDOS through command line over SSH or through DD System Manager, a browser-based graphical user interface.

Multiple DD series appliances can be managed and monitored through a single interface, PowerProtect DD Management Center, or DDMC. Customizable dashboards provide visibility into aggregate status, status by geo, and the ability to drill-down to system-level details. With DDOS 7.5, DDMC can now provide insights into current and projected capacities at the system level for DD series and legacy Data Domain systems allowing for enhanced forecasting and capacity management. Role-based access allows different levels of access via assigned user roles for various levels of expertise within the organization. Simple programmability as well as SNMP monitoring provides additional management flexibility. DDMC offers a pre check option before scheduling a DDOS upgrade to make sure your environment is compatible with the update. Once the pre check is complete you can schedule a one to many upgrade allowing you to schedule multiple DDOS upgrades as opposed to one to one updates. Configuring multiple DD series appliances is simple with DDMC by allowing you to create and apply configuration templates to your appliances. With cyber-attacks and threats on the rise, DDMC can provide compliance alerts when a system's configuration is out of compliance. In the event of a DDOS upgrade failure the appliance will automatically default back to the previous OS release minimizing system downtime and allowing for continuous backup operations.

In addition, DD series has an automatic call-home system reporting called auto-support, which provides email notification of complete system status to Dell EMC support and a selected list of administrators. This non-intrusive alerting and data collection capability enables proactive support and service without administrator intervention, further simplifying ongoing management.

DD series appliances are now integrated with Dell EMC CloudIQ. CloudIQ provides proactive insights and performance analytics across supported storage, data protection, and hyper-converged products through one UI.

DD series software add-ons

DD Boost

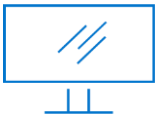
DD Boost software delivers an advanced level of integration with backup applications and data base utilities, enhancing performance and ease of use. Dell EMC also provides a DD Boost File System Plug-In (BoostFS) with DD Boost for even greater application support, which enables all the benefits of DD Boost for applications that use NFS for data protection. Rather than sending all data to the system for deduplication processes, DD Boost enables the backup server or application client to send only unique data segments across the network to the system.

DD Replicator

DD Replicator software provides automated, policy-based, network-efficient and encrypted replication for disaster recovery and multi-site backup and archive consolidation. DD Replicator software asynchronously replicates only compressed, deduplicated data over the WAN. Cross-site deduplication further reduces bandwidth requirements when multiple sites are replicating to the same destination system. This improves network efficiency across all sites and reduces daily network bandwidth requirements making network-based replication fast, reliable and cost effective. In order to meet a broad set of DR requirements, DD Replicator provides flexible replication topologies, such as full system mirroring, bi-directional, many-to-one, one-to-many, and cascaded.

Dell EMC Future-Proof Program and Dell Technologies APEX

Dell EMC Future-Proof Program is a customer facing program that gives our customers additional peace of mind with guaranteed satisfaction and investment protection through a comprehensive set of world class technology capabilities and programs for future technology changes. DD series participates in this Future-Proof Program. DD series is part of the Dell Technologies APEX program allowing for flexible payment options including pay as you go, pay as you use, and provided as-a-Service offerings.



Learn more about
DD series

Contact a Dell Technologies Expert

SEC 17a-4(f) Compliance Assessment

EMC Data Domain Retention Lock Compliance Software Product

Prepared by **Cohasset Associates, Inc.**

Abstract

This technical report is a compliance assessment of the Data Domain Retention Lock Compliance software product capabilities relative to the requirements and conditions of SEC Rule 17a-4(f).

Cohasset's conclusion is that the EMC Data Domain Retention Lock Compliance software meets the relevant requirements of SEC 17a-4(f) in that during the SEC required retention period it: a) provides the integrated control codes and record file management capabilities that ensures protection of record files from overwrite or erasure; b) provides for initial and ongoing accuracy and quality of the stored records, c) uniquely identifies each record file and duplicate copy, and d) provides for a duplicate copy of the record files and recovery from the duplicate copy if required.

Cohasset Associates

3806 Lake Point Tower
505 N. Lake Shore Drive
Chicago, IL 60611 USA

www.cohasset.com

312-527-1550

1.0

Table of Contents

1. Introduction

This section sets the context for this technical assessment. It identifies a) the SEC's regulatory foundation for allowing e-records to be retained on a variety of electronic storage media, and b) the storage system that is the subject of Cohasset's assessment against these SEC electronic storage media regulations.

1.1 The Electronic Storage Requirements of the Securities & Exchange Commission for 17a-4 Records

Records retention requirements for the U.S. securities broker-dealer industry are stipulated by the Securities & Exchange Commission ("SEC") Regulations 17 CFR 240.17a-3 and 17 CFR 240.17a-4 (the "Rule" or "Regulation"), adopted on February 12, 1997. Within this regulation, Rule 17a-4(f) expressly allows records to be retained on electronic storage media, subject to meeting certain conditions.

Three foundational documents collectively define and interpret the specific regulatory requirements that electronic storage systems must meet in order to be SEC compliant under Rule 17a-4(f). They are:

- The Rule itself,
- SEC Interpretive Release No. 34-44238, *Commission Guidance to Broker-Dealers on the Use of Electronic Storage Media under the Electronic Signatures in Global and National Commerce Act of 2000 with Respect to Rule 17a-4,* dated May 1, 2001 (the "2001 Release"), and
- SEC Interpretive Release No. 34-47806, *Electronic Storage of Broker-Dealer Records,* dated May 7, 2003 (the "2003 Release").

In the Rule and the two subsequent interpretative releases, the SEC clearly states that the use of electronic storage media and devices, to the extent that they can deliver the prescribed functionality, satisfy the stipulations of Rule 17a-4.

Rule 240.17a-4(f) specifically states:

> *The records required to be maintained and preserved pursuant to § 240.17a-3 and § 240.17a-4 may be immediately produced or reproduced on "micrographic media" (as defined in this section) or by means of "electronic storage media" (as defined in this section) that meet the conditions set forth in this paragraph and be maintained and preserved for the required time in that form [emphasis added].*
>
> *(1) For purposes of this section:*
>
> * * * * *
>
> *(ii) The term electronic storage media means any digital storage medium or system and, in the case of both paragraphs (f)(1)(i) and f(1)(ii) of this section, which meets the applicable conditions set forth in this paragraph (f).*

The 2003 Release further clarifies that implementation of rewriteable and erasable media, such as magnetic tape or magnetic disk, may meet the requirements of a non-erasable, non-rewriteable recording environment – to the extent that they deliver the prescribed functionality and so long as appropriate integrated control codes are in place. The 2003 Release states:

> *A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software control codes.*

The key words within this statement are "integrated" and "control codes." The term "integrated" means that the method used to achieve a non-rewriteable, non-erasable recording environment must be an integral part of the recording hardware and software. The term "control codes" indicates the acceptability of using attribute codes (metadata) that are integral to the hardware and software of the recording process in order to protect against overwriting or erasure of any records.

Examples of integrated control codes that could be applied towards providing a non-rewriteable, non-erasable recording process are:

- A retention period during which records cannot be erased,
- A unique record identifier that differentiates it from all other records, and
- The date/time of recording (the data/time of recording and the unique identifier serve in combination to "serialize" a record).

The 2003 Release specifically notes that recording processes or applications which merely mitigate the risk of overwrite or erasure (rather than prevent them), such as relying on access control security, will not satisfy the requirements of Rule 17a-4(f).

An important associated requirement of Rule 17a-4(f)(2)(i) is that a member, broker or dealer wanting to store their 17a-3 and 17a-4 records electronically must notify its "examining authority" ninety (90) days prior to employing any technology other than WORM optical media. Examining authorities are self-regulatory organizations (SROs) under the jurisdiction of the SEC such as the New York Stock Exchange (NYSE) and Financial Industry Regulatory Authority (FINRA).

1.2 Data Domain Retention Lock Compliance Software Product Overview

Data Domain offers a product named Retention Lock which can be applied to any Data Domain Managed Tree (a logical volume in a virtual file system). When a Managed Tree is enabled to support Retention Lock, a retention period can be set for individual record files that prevent the record file from being deleted before the retention period has expired. The Retention Lock capability can be configured with two types of software licenses: 1) a Retention Lock Compliance software product license ("Retention Lock Compliance software product") that is designed to meet the requirements of SEC Rule 17a-4(f) and 2) a Retention Lock Governance software product license where certain administrative functions may be performed that are not SEC compliant. This assessment report focuses solely on the Retention Lock Compliance software product license capabilties.

1.3 Assessment and Technical Report

To obtain an independent and objective assessment of the Retention Lock Compliance software product capabilities relative to meeting the requirements set forth in SEC Rule 17a-4(f), EMC Data Domain ("Data Domain") engaged Cohasset Associates, Inc. ("Cohasset"), a highly respected consulting firm with specific knowledge, recognized expertise and more than
30 years of experience regarding the legal technical and operational issues associated with the records management practices of companies regulated by the SEC and SROs.

Cohasset's assignment was to:

- Assess the ability of the Retention Lock Compliance software product capabilities to meet the requirements of all the relevant conditions of Rule 17a-4(f), and
- Prepare this technical report regarding that assessment.

This assessment represents the professional opinion of Cohasset Associates and should not be construed as an endorsement or rejection by Cohasset of the Retention Lock Compliance software

product and its capabilities or other Data Domain products. The information utilized by Cohasset to conduct this assessment consisted of: a) oral discussions, b) system requirements documents, c) user guides, and d) other directly related materials provided by Data Domain.

This assessment covers only the four requirements stated in SEC 17a-4(f) that relate directly to the recording, storage and retention management of regulated record files. The member, broker or dealer must ensure, however, that a combination of procedures, client application capabilities and the storage management capabilities addressed in this assessment meet all seventeen requirements of the Rule.

Additional information about Cohasset Associates is provided in Section 3 of this report.

The content and conclusions of this assessment are not intended and should not be construed as legal advice. Relevant laws and regulations are constantly evolving and legal advice must be tailored to the specific circumstances of the laws and regulations for each organization. Therefore, nothing stated herein should be substituted for the advice of competent legal counsel.

2. Compliance Assessment with SEC Rule 17a-4(f)

This section presents Cohasset's assessment of the Data Domain Retention Lock Compliance software product capabilities that are relevant to meeting the electronic records storage requirements of SEC Rule 17a-4(f).

2.1 Structure and Organization of Cohasset's Assessment

The assessment of each relevant requirement in Rule 17a-4(f) is structured into four parts:

Compliance Requirement – Definition of the specific SEC regulatory requirements that must be met in order to utilize electronic records storage media in the retention of 17a-3 and 17a-4 records;

Compliance Assessment – Cohasset's assessment of the degree to which Retention Lock Compliance software product capabilities comply with the Rule;

Retention Lock Compliance Software Product Capabilities – Description of the Retention Lock Compliance software product capabilities that enable them to meet the specific 17a-4(f) requirement; and

Other Considerations – Identification of actions (if any exist) that may need to be performed in order to meet the requirements of the Rule.

Note: The term "record" is utilized in SEC Rules 17a-3 and 17a-4 to describe all information content that must be retained under the Rules. Since this assessment deals with the capabilities of the Retention Lock Compliance software product relative to SEC Rules, Cohasset Associates has chosen to use the term "record" or "record file" (versus "file") in order to be consistent with SEC terminology.

2.2 Non-rewriteable, Non-erasable Format

2.2.1 Compliance Requirement 17a4(f)(2)(ii)(A)

Preserve the records exclusively in a non-rewriteable, non-erasable format.

As set forth in Section III (B) of the 2001 Release, this requirement "is designed to ensure that electronic records are capable of being accurately reproduced for later reference by maintaining the records in unalterable form."

The following statement in the 2003 Release further clarifies that certain implementations of rewriteable and erasable media, such as magnetic disk or magnetic tape, would meet the requirements of a non-erasable, non-rewriteable recording environment provided a) they deliver the prescribed functionality and b) that functionality is delivered via appropriate integrated control codes for the SEC designated retention schedule associated with the stored record:

> *A broker-dealer would not violate the requirement in paragraph (f)(2)(ii)(A) of the rule if it used an electronic storage system that prevents the overwriting, erasing or otherwise altering of a record during its required retention period through the use of integrated hardware and software control codes.*

2.2.2 Compliance Assessment

It is Cohasset Associates' opinion that the Retention Lock Compliance software product provides very strong capabilities for meeting this requirement of the Rule, provided certain capabilities discussed below are properly configured and applied by the member, broker or dealer and that any conditions stated in subsection 2.2.4, "Other Considerations" are met.

2.2.3 Retention Lock Compliance Software Product Capabilities

The main features of the Retention Lock Compliance software product that support meeting the non-rewritable and non-erasable requirement of the Rule are:

- The member, broker or dealer must purchase unique Retention Lock Compliance software product licenses, as required, which ensure that the "compliance" features of Retention Lock are activated.
- During administrative setup of the Retention Lock Compliance software product, one or more Managed Trees can be defined as being under Compliance control, thereby allowing retention management to be applied to recorded files.

- After a Managed Tree has been configured with Retention Lock Compliance software product it cannot be disabled, overridden or deleted.
- For a Managed Tree that is Retention Lock Compliance software product enabled, a new record file can be placed under Retention Lock Compliance software product control and a time-based[1] retention expiration date set. The time-based retention expiration date is set when the client application, e.g., an e-mail archiving application or file archiving application a) issues a file protocol instruction with an "atime"[2] retention attribute (the retention period) that is set into the future (beyond the date/time of recording) and b) where the retention expiration date is greater than the Minimum defined retention period and less than the Maximum defined retention period. The following situations result in an error condition:
    - If the atime retention expiration date supplied by the client application is less than the current date/time, less than the Minimum retention period per Managed Tree or greater than the Maximum retention period, then an error condition will be returned to the client application.
    - If an attempt is made to delete a record file where the retention period has not expired, then the delete command is rejected and results in an error condition.
    - If an attempt is made to delete a Managed Tree that is Retention Lock Compliance software product enabled and currently contains locked record files with unexpired retention periods, then the delete command is rejected and results in an error condition.
- When an atime retention expiration date has been set for an individual record file, it cannot be deleted or overwritten until the retention period expires. Once the retention period has expired, deletion of the record file may only be performed by a client application, not by a system administrator.
- A Minimum and Maximum time-based retention period for each Managed Tree must be established during the administrative setup of a Retention Lock Compliance software product. This ensures that the atime retention expiration date for a record is not set below the Minimum or above the Maximum. Once set, the Minimum and Maximum retention periods cannot be reduced; they can only be extended.
- The retention expiration date for a record file under Retention Lock Compliance software product control may be extended by recording a new atime retention attribute for the record file that is later in time than the current retention expiration date and less than the Maximum retention.

- An existing retention expiration date cannot be reduced. The Retention Lock Compliance software product will return an error condition to the client application when the new atime retention expiration date is earlier in time than the current atime retention expiration date.
- A Compliance Managed Tree cannot be deleted under any circumstances.
- When a Retention Lock Compliance software product license is un-installed, has expired or is cancelled for any reason, no new Compliance Managed Trees can be defined. However, all of the record files in all existing Compliance Managed Trees will continue to be protected in accordance with the SEC Rule. Also any new files that are stored in existing Compliance Managed Trees with a retention period later than the date stored will be protected in a manner compliant with the SEC Rule.
- Additional administrative security is provided in the Retention Lock Compliance software product to ensure that certain administrative functions or actions that could potentially compromise the integrity of record files prior to expiration of the retention period are not under the control of just one administrative person. This additional administrative security is provided in the form of a dual sign-on, i.e., sign-on by the regular system administrator plus the requirement for second sign-on by an authorized person. Data Domain refers to this feature as the "Security Officer" sign-on (see 2.2.4 Other Considerations). The primary administrative actions that require a dual or Security Officer sign-on in a Retention Lock Compliance software product are:
    - Extending Minimum or Maximum retention periods.
    - Renaming an Managed Tree.
    - Deleting a Retention Lock Compliance software product license.
    - Other system support or maintenance actions that could potentially compromise the integrity of stored record files where the retention period has not expired.
- The accuracy of the system clock in a Retention Lock Compliance software product is critical for determining whether the retention expiration date of a record file has expired. Situations can occur, such as a power outage, maintenance downtime, etc., which may affect the accuracy of the system clock and require it to be adjusted or reset. Additional statistics are gathered, analyses are performed and certain restrictions are placed on ensuring the accuracy of the system clock to meet retention compliance requirements.
    - The accuracy of the system clock and variations of the system clock with current actual time is regularly monitored.

  - The system clock is only allowed to vary by a maximum of two weeks in a year.
  - Should the system clock vary beyond the two week maximum during a year, then the administrative Security Officer dual sign-on is required to reset the clock to current time.

- No logical access (via a software user interface) without Security Officer dual sign-on is allowed for error correction purposes such as the scenario where the Retention Lock Compliance software product experiences a system error or corruption. For the extreme scenario where the full Data Domain operating system will not start up, a restart of the operating system is restricted to single user access via the use of a USB drive which must be physically protected and made accessible only with a second authorization by a Compliance Officer or Security Officer.
- An Managed Tree that is configured as Retention Lock Compliance software product can store files that are not regulated as records under the Rule and, as such, do not require a retention period to be set. Therefore, record files required to be compliant with the Rule as well as non-regulated files can be intermixed on the same Retention Lock Compliance software product Managed Tree (see *2.2.4 Other Considerations*).

2.2.4 Other Considerations

The following actions should be undertaken to ensure that the compliance features of the Retention Lock Compliance software product are activated and configured to meet the requirements of the Rule:

- The member, broker or dealer must purchase a unique Retention Lock Compliance software product license which ensures that the features of the Retention Lock Compliance software product necessary to meet the requirements of the Rule are applied.
- Where administrative functions require a dual or second sign-on (Security Officer sign-on), Cohasset Associates strongly recommends that the authorized second sign-on person be the equivalent of either a Chief Compliance Officer or a Chief Security Officer or their representative as designated in writing.
- It is imperative that the member, broker or dealer insure that the client application which is writing record files regulated under the Rule sends the appropriate retention period for each record file to the Retention Lock Compliance software product.

2.3 Verify Automatically the Quality and Accuracy of the Recording Process

2.3.1 Compliance Requirement 17a-4(f)(2)(ii)(B)

Verify automatically the quality and accuracy of the storage media recording process.

The intent of SEC Rule 17a-4(f)(2)(ii)(B) is to ensure that the media recording process is accurate to a very high degree and, therefore, the recorded information is of the highest quality. The objective of this subsection of the SEC Rule is to provide the utmost confidence that all records read from the storage media are precisely the same as those recorded.

2.3.2 Compliance Assessment

Cohasset believes that the Retention Lock Compliance software product provides exceptional capabilities for meeting the SEC requirement to verify the accuracy and completeness of the recording process.

2.3.3 Retention Lock Compliance Software Product Capabilities

The Retention Lock Compliance software product employs a comprehensive Data Invulnerability Architecture for enhanced data integrity and recoverability. The Data Invulnerability Architecture provides for end-to-end verification using the following capabilities: immediate read back and verification at the time of recording, fault avoidance and containment, continuous fault detection and correction, and file system and Managed Tree recoverability. The capabilities of the Retention Lock Compliance software product that directly support the verification of the quality and accuracy of the recording process are:

Initial Recording Process

- The Retention Lock Compliance software product provides an exceptionally strong capability for verifying quality and accuracy in that for each container of record file data that is written, an immediate read back is performed and the accuracy of the recording is verified before being accepted as error-free. This method goes beyond the minimum acceptable reliance on state-of-the-art magnetic disk recording error checking and detection/correction capabilities.

Post Recording Process

- Record file data is packaged and written in containers (multi megabyte units). A strong checksum value is calculated from the data in each container and stored with that container. The write verification process involves reading back the data in the stored containers and verifying that the checksums are accurate. After the containers are verified, the files contained in them are verified by reading the metadata of the files and verifying that each segment of a file exists in the containers identified by the metadata.
- During read back of a record file, whether by the client archiving application or by the Data Domain file system, the checksums are verified and, when errors are encountered, RAID 6 error correction is applied as required thereby ensuring that the record remains complete and accurate.
- During verification, if the container cannot be recovered using RAID 6, an alert is raised to the client application whereupon the administrative support personnel can recover the data from a replicated or duplicate copy.
- Periodic "scrubbing" of the record file data on the Retention Lock Compliance software product is performed to find and correct any defects that may occur. This is particularly important for those record files that have not been read back for an extended period of time.

2.3.4 Other Considerations

There are no other considerations related to this requirement.

2.4 Serialize the Original and Duplicate Units of Storage Media

2.4.1 Compliance Requirement 17a-4(f)(2)(ii)(C)

Serialize the original, and, if applicable, duplicate units of storage media, and time-date for the required period of retention the information placed on such electronic storage media.

This requirement, according to Section III(B) of the 2001 Release, "is intended to ensure both the accuracy and accessibility of the records by indicating the order in which records are stored, thereby making specific records easier to locate and authenticating the storage process."

While this requirement is thought to be more pertinent to tracking the individual units of removable media related to micrographic or optical storage, the SEC Rule may be satisfied for electronic records by capturing index or metadata associated with each record file that: a) "uniquely" identifies the record file, and b) associates a "date of recording" with each record file.

2.4.2 Compliance Assessment

Cohasset believes that Retention Lock Compliance software product meets the SEC requirement to serialize both the original record and each duplicate copy stored.

2.4.3 Retention Lock Compliance Software Product Capabilities

The following capabilities of the Retention Lock Compliance software product are designed to meet the requirement of the Rule.

- The Retention Lock Compliance software product identifies each record file with a unique user ID which contains a unique file name and date/time recorded stamp, thereby uniquely identifying each record file logically and chronologically.
- When record files managed under the Retention Lock Compliance software product are replicated to another Data Domain system with the Retention Lock Compliance software product, the unique file name and data/time stamp as well as all retention metadata attributes are duplicated.

2.4.4 Other Considerations

There are no other considerations related to this requirement.

2.5 Store Separately a Duplicate Copy

Compliance Requirement 17a-4(f)(3)(iii)

Store separately from the original a duplicate copy of the record stored on any medium acceptable under 240.17a-4 for the time required.

The intent of this requirement is to provide an alternate storage source for accessing the record should the primary source be compromised, i.e., lost or damaged.

Note: A "duplicate copy" is different from a backup copy in the sense that the duplicate copy is the recording of a real-time copy of the record or recording a one-for-one "journal" copy of the record that is never overwritten or erased. Backup copies, on the other hand, may be overwritten as they are "rotated" on a periodic basis.

2.5.2 Compliance Assessment

It is Cohasset's opinion that Retention Lock Compliance software product complies with this SEC requirement.

2.5.3 Retention Lock Compliance Software Product Capabilities

- The Retention Lock Compliance software product provides for an Managed Tree to be replicated to a second Retention Lock Compliance software product Managed Tree, either locally or remotely. During Replication, all record file data and associated metadata, including retention metadata, are replicated to the second file system or Managed Tree.
- Should a major error occur that makes the original file system or Managed Tree inaccessible, then the record files can be recovered from the replicated copy of the Managed Tree.

2.5.4 Other Considerations

There are no other considerations related to this requirement.

3. Conclusions

This technical assessment has addressed whether the Retention Lock Compliance Storage System capabilities meet the requirements and conditions of SEC Rule 17a-4(f).

Cohasset's opinion is that the Retention Lock Compliance Storage System:

- Meets the requirements of the Rule for preserving the records in a non-erasable, non-rewriteable format through the use of integrated control codes and records retention management functionality.
- Meets the requirements of the Rule related to the automatic verification of the accuracy and quality of the recording process in that it employs a comprehensive Data Invulnerability Architecture that immediately reads back and verifies each container of record file data stored, and utilizes state-of-the-art error detection and RAID 6 technology to correct any errors detected during read-back and periodic scrubbing.
- Uniquely identifies and serializes each record and duplicate copy that is stored.
- Supports storing a compliant duplicate copy of each record and provides for the recovery of record files from the duplicate copy.

Cohasset Associates' conclusion: The Retention Lock Compliance Storage System meets all of the SEC requirements that are its direct responsibility for retaining and storing in digital form 17a-3 and 17a-4 records – pursuant to all the requirements set forth in Rule 17a-4(f), which expressly allows records to be retained on electronic storage media.

End Notes

1. Retention Lock currently supports only time-based retention (i.e., retained for a specified period from the time after the file is recorded). Event-based retention (i.e., indefinite retention once the file is recorded until a specified event occurs, followed by a fixed, final retention period) is not currently supported.

2. The "atime" attribute in standard file protocol instructions represents the "time last accessed" for a file. For Retention Lock Compliance software enabled Managed Trees, this attribute is utilized to establish the retention expiration date for a record file.

3. Redundant Array of Independent Disks (RAID): A method for recording data to magnetic disk devices that provides for various levels of error correction and read or write performance improvements. RAID 6 employs striped disks with dual parity and combines four or more disks in a way that provides for correction of detected errors for up to as many as two full disk units of data during read back.

About Cohasset Associates, Inc.

Cohasset Associates, Inc. (www.cohasset.com), is one of the nation's foremost consulting firms specializing in records and information management. Now in its fourth decade of serving clients throughout the United States, Cohasset Associates provides award-winning professional services in three areas: management consulting, education and legal research.

Management Consulting: The focus of Cohasset Associates' consulting practice is improving the programs, processes and systems that manage document-based information. Cohasset works to provide its clients with cost-effective solutions that will both achieve their business objectives and meet their legal/regulatory responsibilities. This ranges from establishing effective corporate records management programs to planning state-of-the-art electronic records systems.

Education: Cohasset Associates is renowned for its longstanding leadership in records management education. Today, Cohasset's educational work is centered on its annual National Conference for Managing Electronic Records (MER), which addresses the operational, technical and legal issues associated with managing the complete life cycle of electronic records (www.merconference.com). The MER sessions also are available at RIM on Demand. (www.rimeducation.com/videos/rimondemand.php)

Legal Research: Cohasset Associates is nationally respected for its leadership on records management legal issues – from retention schedules to the use of alternative media to paper for storing document-based information.

For more than twenty years, Cohasset Associates has been a "thought leader" in records and information management. Cohasset has been described as the only management consulting firm in its field with its feet in the trenches and its eye on the horizon. It is this blend of practical experience and a clear vision of the future that, combined with Cohasset Associates' commitment to excellence, has resulted in Cohasset Associates' extraordinary record of accomplishments and innovation.

DD OS, PowerProtect DD Virtual Edition, and PowerProtect DD Management Center

Security Configuration Guide

7.5

February 2021
Rev. 01

DELL EMC

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

Contents

Revision history

The following table presents the revision history of this document.

Table 1. Publication history

Revision	Date	Description
01 (7.5.0.5)	February 2021	Updates include: ● FTPS inbound communication port ● MFA for sysadmin and security-officer authorization ● FTPS configuration recommendation for TLS-version and cipher-list

1

Overview

This chapter includes:

Topics:

DD OS

Data Domain and PowerProtect systems are appliances that run the DD OS. A web-based user interface (UI), DD System Manager, is provided for configuration operations, management, and monitoring. In addition, a controlled command-line interface (CLI) environment is available, which provides a complete set of administrative operations.

Because DD OS is an embedded operating system, additional software or agents cannot be installed or run within a system. This restriction ensures control and consistency of DD OS releases and provides additional security over the system.

Data Domain and PowerProtect systems are purpose-built physical and virtual appliances with restricted access to their internal operation. Any tampering voids the warranty. Updated versions of embedded open-source modules are in DD software updates as appropriate.

DD system security

Data Domain and PowerProtect systems, as central repositories for both structured and unstructured backup data, have many security capabilities and attributes to protect the data. This document is a supplement to the *DD OS Administration Guide* and provides an overview of key security features and procedures that are required to ensure data protection and appropriate access control.

DD OS system interfaces and access control

Hosts and backup applications interface with the Data Domain and PowerProtect systems through one or more of the standard native server interface protocols: CIFS, NFS, NDMP, VTL, or DD Boost.

Access control and user authentication to the system is controlled by either local users, NIS environments, LDAP, Kerberos authentication, or within a Microsoft Active Directory Domain environment. Other points that run the security attributes of the system are listed in the simplified diagram.

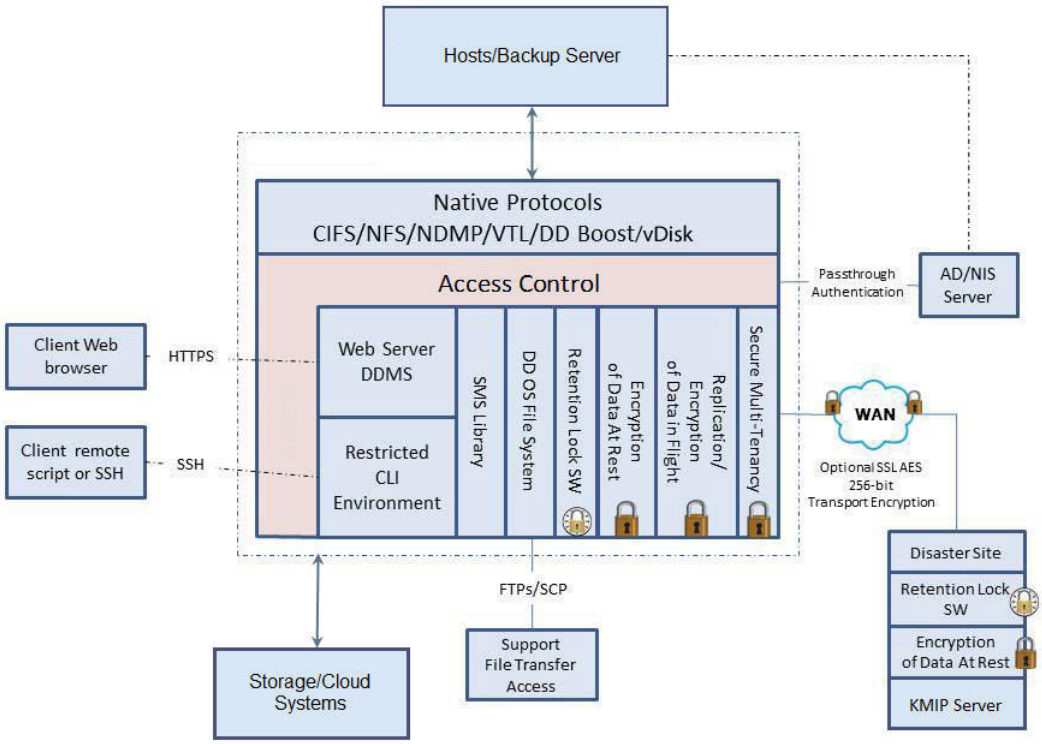


Figure 1. System interfaces and access control

The following native protocols and software options depend on or enable security attributes of the system. See the current *DD OS Administration Guide* for more information.

Supported Native Ingest Protocols

DD and PowerProtect systems support simultaneous access through common network access protocols, enabling both backup servers and application servers to send data to the system. Servers can attach and transfer files and backup images over one or more of these protocols:

- CIFS
- NFS
- Data Domain Boost over IP (encryption supported)
- Data Domain Boost over Fibre Channel (encryption not supported)
- NDMP
- VTL over Fibre Channel
- vDisk over Fibre Channel

Data that is transmitted over CIFS, NDMP, DD Boost over Fibre Channel, VTL over Fibre Channel, and vDisk over Fibre Channel is transported unencrypted.

The following software options that are highlighted below are related to security and require separate licenses.

DD Replicator Software

Automated, policy-based, network-efficient replication for disaster recovery, remote office data protection, and multi-site tape consolidation. DD Replicator software asynchronously replicates only the compressed, deduplicated data over the WAN or LAN during the backup process, making network-based replication fast, reliable, and cost-effective.

For environments that do not use a VPN for secure connections between sites, DD Replicator software can securely encapsulate its replication payload over SSL with AES 256-bit encryption for secure transmission over the wire. This process is also known as encrypting data in flight.

DD Encryption Software

Protects backup and archive data that is stored on systems with data encryption that is performed inline before the data is written to disk. The Encryption at Rest feature satisfies internal governance rules, compliance regulations, and protects against the reading of customer data on individual disks or disk shelves that are removed from the system due to theft.

DD Retention Lock Software

Prevents specified files from being overwritten, modified, or deleted for a user-defined retention period of up to 70 years.

DD Secure Multi-Tenancy Software

Provides secure storage consolidation in multi-tenant backup environments. With SMT, multiple tenants can reside on a single system simultaneously and the data of one tenant cannot be detected or accessed by another.

DDMC interfaces and access control

PowerProtect DD Management Center (DDMC) permissions can be assigned to system groups, systems, and users.

The user permissions for DDMC are by assigned roles and have three components:

- the managed object (groups or systems)
- the user (local, NIS, or Active Directory)
- the DD System Manager role (Administrator, Limited-Admin, Backup Operator, or User)

NOTE: The Backup Operator only exists in assigning role to the system, not for a role in DDMC.

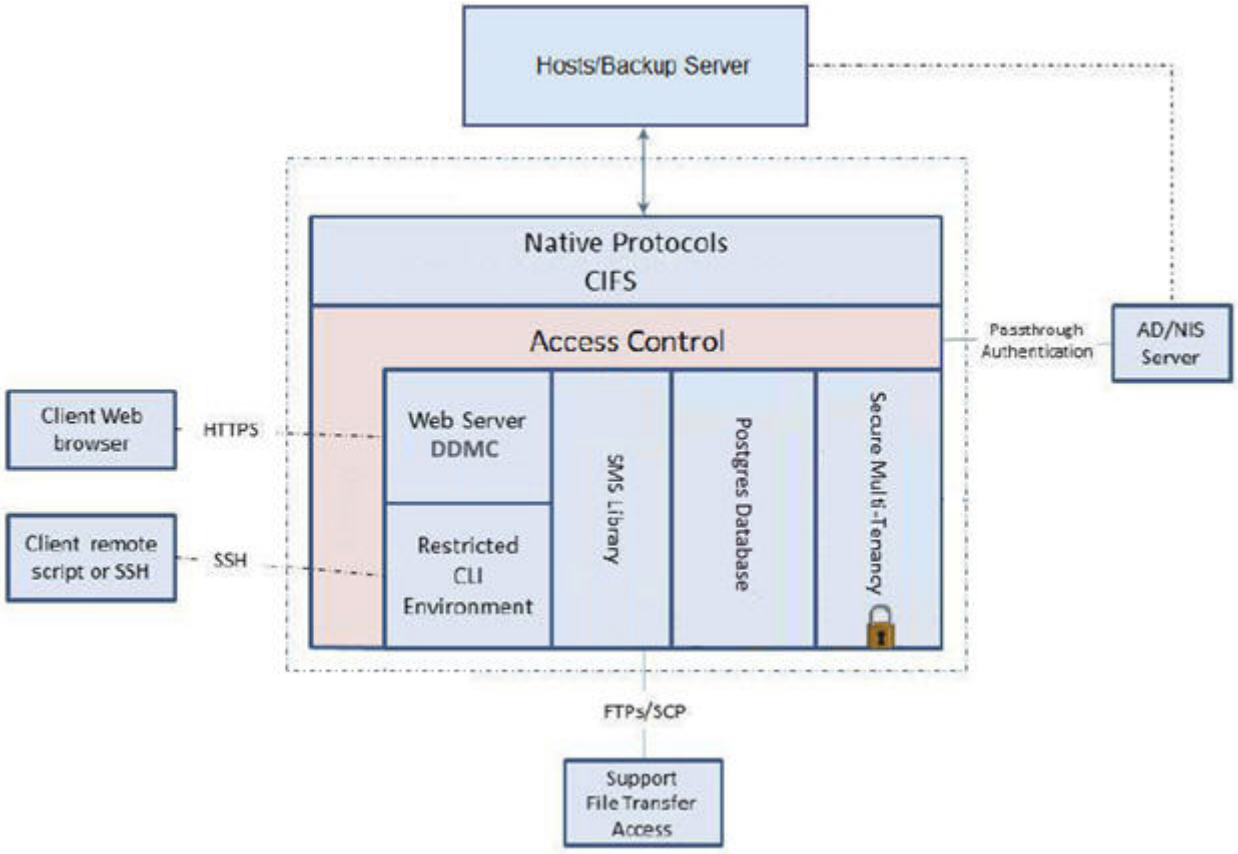


Figure 2. DDMC interfaces and access control

- A user's role is determined by the highest (most privileged) role that is assigned to any group the user belongs to. If a user belongs to a group that has an admin role but the user itself is only assigned a backup role, the user's role will be admin because of its membership in the group. Another scenario is if a user belongs to two AD groups that are assigned to the same system DD1. If Group "A" is assigned the admin role on DD1 and Group "B" is assigned the backup role on DD1, then the user's role for DD1 will be admin due to Group "A" having the admin role.
- This system role enables a DDMC user to create tenants and tenant units based on system permissions.
- DDMC user can also create reports based on the system role.
- DDMC user can also launch DD System Manager with this assigned role; however, DDMC user and system user are not the same.
- A sysadmin in DDMC is considered a different user than a sysadmin user on a DD or PowerProtect system.

2

Security Configuration Settings

This chapter includes:

Topics:

Introduction

This chapter provides an overview of the settings available to ensure the secure operation of the product.

System passphrase

The system uses the passphrase to encrypt the encryption keys, cloud access, secure keys, imported host certificate private keys, and DD Boost token keys. It enables a system to be transported with encryption keys on the system but without the passphrase being stored on it. If the system is stolen in transit, an attacker cannot easily recover the data, and at most, they can recover the encrypted user data and the encrypted keys.

Data at rest encryption keys are dependent on this passphrase, and therefore, the use of a stronger passphrase is mandatory. A valid passphrase must contain:

- A minimum of nine characters
- A minimum of one lowercase character
- A minimum of one uppercase character
- A minimum of one numeral
- A minimum of one special character
- No spaces

DD OS supports passphrase up to 254 characters.

DDMC only uses a passphrase for imported host certificate private keys.

For more information, see the *DD OS Administration Guide* or *DDMC Installation and Administration Guide*.

Passphrase security

The passphrase is encrypted and stored in a file on the head unit of the DD system. The encryption key that is used to encrypt the passphrase is hardcoded.

Users can choose to not store the passphrase on disk. There is a hidden sysadmin command to accomplish this task: `system passphrase option set store-on-disk no`.

NOTE: If the system is configured to not store the passphrase, there is no way to recover it if it is lost.

Change the passphrase after running the command to not store the passphrase on disk. A side-effect of not storing the passphrase is that the file system has to be unlocked every time that the system is rebooted. Until the file system is unlocked, all backup jobs and replication are impacted.

NOTE: If multifactor authentication is enabled, the security officer must enter an RSA SecurID token after their password.

NOTE: If there is no concern that an attacker can gain physical access to the appliance in the environment, then choose to store the passphrase on disk.

For more information, see the *DDOS Administration Guide* and *DDOS Command Reference Guide*.

Access control settings

Access control settings enable the protection of resources against unauthorized access.

System access

The Data Domain and PowerProtect operating environment provides secure administration through either the DD System Manager by HTTPS or SSH for CLI. Either method enables locally defined users, Network Information Service (NIS) users, Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory (AD) domain users, and Single Sign-on (SSO).

DD System Manager over HTTPS

The system can use an imported certificate to establish a trusted connection to manage the system over SSL. If a certificate is not provided, the system can use its self-signed identity certificate. HTTPS is enabled by default.

When connecting to DD System Manager from a web browser, all HTTP connections will automatically redirect to HTTPS.

NOTE: HTTP can only be enabled through the UI or CLI.

SSH for CLI

The administrator enters a controlled shell environment, where individual CLI commands manage the system.

NOTE: When connecting to an HA system using the floating hostname or IP using an SSH client, the public key that is stored in the known-hosts list of the local shell may fail verification. Each node in the HA pair generates a unique SSH key pair, and the active node presents the key that it owns. Resolution for this issue is to physically verify that the correct system is connecting, and remove the offending key in the known-host list and revalidate the key on the next connection try. Knowledge Base article #212538 explains this issue in more detail.

Administrative system access can be either *local* or *remote*.

To log in using SSH, minimum SSH version that is supported is OpenSSH v4.7p1.

To login with FIPS enabled using SSH, minimum SSH version that is supported is OpenSSH v5.9p1.

Local access

Authorized administrators with valid login credentials have access to CLI through serial console or IP in same subnet. User is prompted for username and password, and after authentication and authorization, they are granted login access.

Remote access

CLI and Web-based System Manager remote access are available for authorized administrators with proper login credentials (username and password). Remote users with network access and authorization

can remotely administer the systems over the network. Policies outside the system should be put in place for users to log out after the session is over for both local and remote access.

Password-less login is supported for SSH using SSH keys and for DD System Manager and REST API connections by using client certificates.

NOTE: SSH and secure browsing (HTTPS) are enabled by default. The recommendation is to use an imported certificate and to configure session timeout values to ensure that users are automatically logged out of the system after the session is over. A session timeout of 5 minutes maximum is recommended.

Host-based access lists

Data is not readily viewable from anywhere except a host that has been granted access. Administrator access is required to configure the Data Domain system and adjust which physical hosts can view an exported mount point. Users with administrative access can update the access list with a server's hostname or IP address. A system can use DNS for name resolution.

For greater protection, administrators can use the CLI `net hosts add <ipaddr> <host-list>` to add entries in the hosts file to control host resolution. See the *DD Command Reference Guide* for more information.

File permissions

Files that are created on the Data Domain system are "owned" by the creator. For example, backup software typically writes files as a particular user, so that user would own all files that the backup software created on the system. Explicit permissions (ACLs) must be set, however, to prevent users from viewing files created by others.

Microsoft CIFS

For every file or folder that is created through CIFS, the following attributes are created:

- Owner SID
- Group SID
- DACL (Discretionary ACL – Permissions)
- SACL (System ACL – Auditing Information)
- DOS Attributes such as READONLY, HIDDEN, SYSTEM & ARCHIVE

Also, folders and files map UNIX UID/GID/MODE from Windows Owner-SID/Group-SID/DACL. The DACL is inherited from its parent. If the parent directory does not have DACL (created though NFS/non-CIFS), then a default ACL is assigned. The default gives the owner full control and gives others read permission. Access control is managed through the standard Microsoft Management Control (MMC) on any client with permissions to do so.

Linux NFS

Files and folders that are created through the remaining ingest protocols use the POSIX.1e ACL standard or NFSv4 native ACLs through the `nfs4_setacl` command. Every object is associated with three sets of permissions that define access for the owner, the owning group, and for others. Each set may contain Read [r], Write [w], and Execute [x] permissions. This scheme is implemented using only 9 bits for each object. In addition to these 9 bits, the Set User Id, Set Group Id, and Sticky bits are used for various special cases. Access control is managed through a standard Linux client or DD OS CLI administration environment with permissions to do so.

DD Boost

Files and directories that are created using DD Boost APIs are created with the mode (or permission) bits specified by the creator. Thus each object is associated with three sets of permissions that define access for the owner, the owning group, and for others. Each set may contain Read [r], Write [w], and Execute [x] permissions. The mode bits can be changed appropriately through a DD Boost change mode API.

Microsoft Active Directory (AD) Services

Data Domain and PowerProtect systems can use Microsoft Active Directory pass-through authentication for the users/servers. Administrators can enable certain domains and groups of users to access files that are stored on the system. It is recommended to have Kerberos configured. Also, systems support Microsoft Windows NT LAN Managers NTLMv1 and NTLMv2. However, NTLMv2 is more secure and is intended to replace NTLMv1.

NIS Directory Services

Data Domain and PowerProtect systems can use NIS Directory Authentication for the users in UNIX/LINUX environments. Administrators can enable specific hosts and users to access files that are stored on the system.

Kerberos Authentication

Kerberos authentication for NFSv3 and NFSv4 clients can be used. Kerberos performs with NIS Directory or LDAP services to identify connecting clients. This authentication method enables the administrator to control which users and hosts have permissions to view data on a system.

NOTE: There is no Kerberos configuration in DDMC.

LDAP for NFS ID mapping	Data Domain and PowerProtect systems can use LDAP for NFSv4 ID mapping, and NFSv3/NFSv4 Kerberos with LDAP. User can also configure Secure LDAP with either LDAPS or Start_TLS method. The LDAP client authentication can use Bind DN or Bind PW, but systems do not support certificate-based LDAP client authentication. **NOTE:** Local user IDs start with the number 500. When setting up LDAP, a similar user ID range (500–1000) cannot be used or a user ID collision occurs. If there is user ID collision, files that are owned by a name LDAP service user become accessible by the other users due to configuration errors.
Separate NFS and CIFS shares	Administrators can easily create shares on the file system. Using the native access control methods helps to define more granular share/directory/file-level access control over certain data on the system. For example, when setting up a shared system for multiple customers, administrators can have an NFS or CIFS share that is created for each specific customer on the same system and specify access controls for each customer/share.
Single Sign-on	SSO enables you to register a DD or PowerProtect system with a supported SSO provider and to use the SSO provider credentials for system-level user authentication. **NOTE:** Data Protection Central (DPC) is the only supported SSO provider. DPC version 19.1 is required to use SSO.

User authentication

User authentication settings control the process of verifying an identity claimed by the user for accessing the product.

Default account

The default user account is *sysadmin*. The account cannot be deleted or modified.

For DD and PowerProtect systems, the factory default password is the serial number of the system. For its location, see the system-specific hardware overview manual.

During the initial configuration, the administrator who logs in to DD OS or DDMC as sysadmin is prompted to change the password. Use a strong and complex password.

For DDVE residing on ESXi, Hyper-V, and KVM, the default password is **`changeme`**. During the initial configuration, the administrator who logs in as sysadmin is prompted to change the password.

For AWS, the default password is the instance id, during the initial configuration, the administrator has to change the password during first login.

For Azure, the user specifies the password during deployment and is not required to change the password.

For GCP, the default password is `changeme`. The administrator is required to change the password during the first login.

NOTE: Change the default password to a more complex and stronger password after logging in to the system for the first time.

DDSH should also ask to create a security officer with the first login. If "yes" is selected, then a username and password for the new security officer must be provided. If "no" is selected, the next steps in initial configuration setup of the system, DDVE, or DDMC will begin.

The creation and assignment of a security officer is highly recommended.

NOTE: When sysadmin is creating the first security officer, sysadmin cannot use the same password as sysadmin's for the first security officer. If sysadmin tries to create a security officer with same password as sysadmin's, the message `Incorrect Password` is displayed.

Multi-factor authentication for sysadmin and security-officer authorization

The system requires additional authorization for certain commands to promote better security and protection, which means sysadmin or security-officer credentials are required to run these commands.

When multi-factor authentication (MFA) enabled on a system, in addition to sysadmin or security-officer credentials, , the system will also ask for MFA passcode for certain commands to promote better security and protection.

An MFA passcode is usually a time-based one-time password (TOTP) that changes every 30 or 60 seconds. Different MFA providers support different ways of generating TOTP, common MFA providers include RSA SecurID, Google Authenticator/ Microsoft Authenticator, and Authy.

DD supports RSA SecurID as MFA provider.

The following CLIs are protected with MFA and require sysadmin or security-officer authorization:

- `filesys destroy`
- `cloud unit del`
- `system sanitize`
- `authentication mfa rsa-securid disable`
- `filesys encryption lock` (also supported through the UI)
- `system passphrase option set store-on-disk no`

Local users

After logging in as sysadmin, you can create additional accounts for the roles that are described in Role-based accounts on page 15. As an admin-role or limited-admin user, you can change a user's role for an account, password, and account expiration parameters. For more information and instructions, or to change just the password for individual users, see the *DD OS Administration Guide*.

For uniform password management across the enterprise, the default password policy can be changed and applied to all newly created passwords with the default policy set. Parameters include the following:

- Minimum Days Between Change
- Maximum Days Between Change
- Warn Days Before Expire
- Disable Days After Expire
- Minimum Length of Password
- Minimum number of Character Classes
- Lowercase Character Requirement
- Uppercase Character Requirement
- One Digit Requirement
- Special Character Requirement
- Max Consecutive Character Requirement
- Number of Previous Passwords to Block
- Maximum login attempts
- Unlock timeout (seconds)

NOTE: DD Boost users and passwords are created using the procedure that is described in the DD Boost chapter in the *DD OS Administration Guide*.

Enabling, disabling, or deleting user accounts

Local user accounts are enabled, disabled, or deleted by the system administrator. For more information and instructions, see the *DD OS Administration Guide*.

Active Directory

Data Domain and PowerProtect systems can use Microsoft Active Directory pass-through authentication for the users. Refer to *DD OS Administration Guide* for active directory configuration.

NIS

Data Domain and PowerProtect systems can use NIS Directory Authentication for the users in UNIX/LINUX environments for configuration management. Refer to *DD OS Administration Guide* for NIS configuration.

LDAP

Data Domain and PowerProtect systems can use LDAP for user authentication. Users can also configure Secure LDAP with either LDAPS or Start_TLS method.

NOTE: Local user IDs start with the number 500. When setting up LDAP, a similar user ID range (500–1000) cannot be used or a user ID collision occurs. If there is user ID collision, files that owned by a name LDAP service user become accessible by the other users due to configuration errors.

Refer to *DD OS Administration Guide* for LDAP and Secure LDAP configuration.

Single Sign-on

Data Domain and PowerProtect systems can authenticate a user with a username and password from a supported Single Sign-on (SSO) provider. SSO feature must be enabled and the system must be registered with an SSO provider. Refer to *DD OS Administration Guide* for more information.

Login using certificates

User certificate consisting of username is authenticated and authorized based on pre-existing role mapping to login to DD System Manager from GUI and REST, see *DD OS Administration Guide* for more information.

User authorization

User authorization settings control rights or permissions that are granted to a user for accessing a resource that manages the product.

Specific authorization levels are defined for each user account created using the Role-Base Access Control scheme that is listed below. To change the authorization for an account, you must change the role that is specified for the account.

Table 2. Role-based accounts

Role/Account Type	Description
admin	An *admin* role user can configure and monitor the entire system. Most configuration features and commands are available only to admin role users. However, some features and commands require the approval of a security role user before a task is completed.
limited-admin	The *limited-admin* role can configure and monitor the system with some limitations. Users who are assigned this role cannot perform data deletion operations, edit the registry, or enter bash or SE mode.
user	The *user* role enables users to monitor systems and change their own password. Users who are assigned the user management role can view system status, but they cannot change the system configuration.
security (security officer)	• A *security* role user, who may be referred to as a security officer, can manage other security officers, authorize procedures that require security officer approval, provide data destruction oversight, and perform all tasks that are supported for security role users. • The security role is provided to comply with the Write-Once-Read-Many (WORM) regulation. Most command options for administering sensitive operations, such as Encryption, Retention Lock Compliance, and Retention Lock Archiving now require security officer approval.
backup-operator	• A *backup-operator* role user has all user role permissions, can create snapshots for MTrees, and can import, export, and move tapes between elements in a virtual tape library. • A backup-operator role user can also add and delete SSH public keys for password-less logins. This function is used mostly for automated scripting. The backup-operator can

Table 2. Role-based accounts (continued)

Role/Account Type	Description
	add, delete, reset and view CLI command aliases, synchronize modified files, and wait for replication to complete on the destination system.
none	The *none* role is for DD Boost authentication and tenant-unit users only. A none role user can log in to a Data Domain system and can change their password, but cannot monitor, manage, or configure the primary system. When the primary system is partitioned into tenant units, either the tenant-admin or the tenant-user role is used to define a user's role for a specific tenant unit. The tenant user is first assigned the none role to minimize access to the primary system, and then either the tenant-admin or the tenant-user role is appended to that user.
tenant-admin	A *tenant-admin* role user can configure and monitor a specific tenant unit.
tenant-user	The *tenant-user* role enables a user to monitor a specific tenant unit and change the user password. Users who are assigned the tenant-user management role can view tenant unit status, but they cannot change the tenant unit configuration.

After other user accounts are created, those user accounts can change their own configuration, but cannot perform configuration changes on other user accounts of the same level.

For more information about user roles and instructions for creating users and viewing user configuration information, see the *DD OS Administration Guide*.

NOTE: For DDMC only admin, limited-admin and user roles are supported. Refer to the *DDMC Installation and Administration Guide* for information about the differences between DDMC and DD System Manager and the RBAC settings for launching the system manager from DDMC.

Certificate management

Data Domain and PowerProtect systems can use certificates to securely communicate with following applications and protocols: HTTPS, external Key Manager (KMIP-compliant key manager such as KeySecure v8.5, v8.9, v8.10, and v8.12.1, NextGen v1.9.1 and v1.10 from Safenet/Gemalto, and Data Security Manager (DSM) 6.3 from Thales/Vormetric), DD Boost, LDAP server, Cloud Tier (AWS, Azure, Alibaba Cloud, Google Cloud, ECS, AWS federal), and certificate-based user authentication and two factor authentication with a Common Access Card (CAC).

Data Domain and PowerProtect systems use self-signed certificates to build mutual trust between another system for secure data replication. It supports two different secure configurations using certificate that is one-way and two-way authentication.

Managing a DD system with DDMC

To manage a Data Domain or PowerProtect system, a trust must be established between DDMC and the system. A self-signed certificate is used to establish the trust. For more information, see the *DDMC Installation and Administration Guide*.

Cloud certificates

The cloud providers have a host certificate that is issued by a CA to verify the identity of a cloud provider before backing up data from a system. Import the CA certificate and any applicable CRLs before backing up any data to the cloud. See details in section Certificates for cloud providers.

Certificate revocation list

A Certificate Revocation List (CRL) is a PEM formatted file that is issued by a Certificate Authority (CA) listing certificates that have been revoked and thus are no longer valid. Once a CRL file is imported to DD System Manager, the revoked certificates in the list can no longer be used to log in to the system. The Online Certificate Status Protocol (OCSP) which dynamically checks a certificate's validity each time it is used, is not supported.

NOTE: Ensure that the CRL has a valid NextUpdate field before importing. It should not be expired.

DD Boost certificates

The DD Boost protocol can be used with or without externally signed certificates for authentication and to provide data encryption. Use of certificates provides a more secure data transport capability. The DD Boost protocol also supports optional encryption when certificates are not used.

In-flight encryption enables applications to encrypt in-flight backup or restore data over LAN from the system. When configured, the client can use TLS to encrypt the session between the client and the system. If TLS with certificates is used, then the specific suites that are used are DHE-RSA-AES128-GCM-SHA256 and DHE-RSA-AES256-GCM-SHA384 for medium and high encryption, respectively. If TLS encryption is used without certificates, the specific suites that are used are ADH-AES128-GCM-SHA256 and ADH-AES256-GCM-SHA384 for medium and high encryption respectively.

HTTPS certificates

The system can use an imported certificate to establish a trusted connection to manage the system over SSL. If a certificate is not provided, the system can use its self-signed identity certificate.

Data encryption certificates

External CA and host certificates are required to set up the KMIP-compliant key manager such as KeySecure v8.5, v8.9, v8.10, and v8.12.1, NextGen v1.9.1 and v1.10 from Safenet/Gemalto, and Data Security Manager (DSM) 6.3 from Thales/Vormetric/Thales. If encryption is enabled on Cloud Tier, only the Data Domain embedded key manager (EKM) is supported.

For information about encryption certificates and key managers, see the Encryption chapter in the *DD OS Administration Guide*.

LDAP certificates

LDAP for NFS ID mapping for folder and file permissions support secure LDAP using certificates.

High Availability

In a High Availability (HA) configuration, there are two controllers, where only one at a time is active, and are logically considered as a single file system.

- Both systems have the same Root Certificate Authority.
- To establish mutual trust with the HA system, trust is required to be established with the active node ONLY.
- Mutual trust, certificate signing request, and all the imported certificates on the active node are mirrored to the standby node.
- Host certificate is generated per Active and Standby node and is used for HTTPS application. CA for secure support bundle upload is also kept per node.

Externally signed certificates

Certificate authority (CA) is in public certificate (PEM) format to establish a trusted connection between the external entity and each system.

If the system uses the external key manager, it requires a PKCS12 host certificate and CA certificate in PEM (public key) format to establish a trusted connection between the external key manager server and each system that it manages.

The certificate signing requires PKCS10 format. The public certificate key can have either PKCS12 (public plus a private key) or PEM format. The host certificate PEM format is used only with the Certificate Signing Request (CSR) feature.

Individual host certificates can be imported for HTTPS and communication with external key manager.

Importing the host certificate in PKCS12 format is supported. If there is a CSR on the system, you can import the host certificate in PEM format after the CSR is signed by a Certificate Authority.

NOTE: The system passphrase is required to import the certificate.

On a FIPS enabled DD system, PKCS12 file must be FIPS-compliant. While encrypting PKCS12 file, compatible encryption algorithms must be used. We recommend using "PBE-SHA1-3DES" for encrypting key and certificate in PKCS12 file.

See the *DD OS Administration Guide* for certificate management configuration.

Log settings

A log is a chronological record of system activities that is sufficient to enable the reconstruction and examination of the sequence of environments and activities surrounding or leading to an operation, procedure, or event from inception to final results.

All system logs (system, space, errors, access related) are stored on the root file system partition, and not accessible directly except through these services:

- Logs can be configured to send to a remote syslog server.
- Authorized service personnel can copy logs to another system via FTP or SCP.
- Some logs can be accessed via successful login via the CLI or the System Manager.

The system log file entries contain messages from the alerts feature, autosupport reports, and general system messages. The log directory is `/ddvar/log`.

For more information, see the *DD OS Administration Guide*.

Log descriptions

Log files can be bundled and sent to Dell EMC Support to provide the detailed system information that aids in troubleshooting any system issues that may arise. The Data Domain system logfile entries contain information from the alerts feature, autosupport reports, bash scripts, and general system messages.

Audit and secure logs are searchable by multiple parameters, such as username, string, authentication failure/successes, including tenant-units. Users who are assigned the "tenant-admin" role on tenant-units can only see the logs for the tenant-units which belong to them. Any configuration changes that were done on the tenant-units that are owned by the tenant-admins are shown.

This table lists logs that are important to system security.

Table 3. Log files

Log name	Location and description
messages	`/ddvar/log/messages` The system log, generated from system actions and general system operations.
audit.log	`/ddvar/log/debug/audit.log` Lists all the CLI commands that are run through DDSH, by user and associated user role. Access to this log is controlled by user roles. System admin users can see all audit logs in the system. Tenant-admin users can see the audit logs for all tenant-units they own.
access_log	`/ddvar/log/debug/sm/access_log` Tracks users of the DD System Manager UI (GUI).
secure.log	`/ddvar/log/debug/secure.log` Messages from successful and unsuccessful logins and logouts, including authentication failures by known and unknown users, as well as changes to user accounts, and any other PAM messages.
cifs.log	`/ddvar/log/debug/cifs/cifs.log` Messages about CIFS-related activity from CIFS clients attempting to connect to the Data Domain system. Messages from the CIFS subsystem are logged only in `cifs.log`.
ddsh.info	`/ddvar/log/debug/sm/ddsh.info` Tracks all commands that are issued by CLI users on the system.
kmip.log	`/ddr/var/log/debug/kmip.log` All KMIP initialization and transactions logs are listed here.

For more information about logs, see the *DD OS Administration Guide*.

Log management and retrieval

See the *DD OS Administration Guide* for the following topics:

- Log roll-over
- Viewing log files from the DD System Manager
- Displaying log files using the CLI
- Understanding and saving log messages
- Sending log messages to another system (configuration of an external Syslog server) - It is recommended to forward system logs to an external server. Logs can still be evaluated if the local system is down or unresponsive.

Additional log management topics are covered in the *DD OS Administration Guide*, as follows:

- To configure CIFS logging levels, see "Setting CIFS Options."
- To configure log alert mechanisms, see "Managing Alert Reporting and Configuration of Alert Mechanisms."

Communication security settings

Communication security settings enable the establishment of secure communication channels between the product components as well as between product components and external systems or components.

TCP and UDP ports

The tables below show input and output ports for TCP and UDP.

Table 4. System inbound communication ports

Service	Protocol	Port	Port Configurable	Default	Description
FTP	TCP	21	No	Disabled	Port is used only if FTP is enabled. Run `adminaccess show` on the system to determine if it is enabled. **NOTE:** Using FTP is not recommended. SCP is recommended for file transfer to and from the DD system. FTPS should be considered before using FTP.
FTPS	TCP	21	No	Disabled	Port used only when FTPS is enabled. Run `adminaccess show` on system to determine if ftps is enabled. **NOTE:** FTPS uses TLS v1.2 by default and cipher-list `ALL:!ADH:!EXPORT56:!EXPORT40:+HIGH:!MEDIUM:!LOW:!SSLv2:!SSLv3:!DES-CBC3-SHA:+EXP@STRENGTH` by default. `adminaccess ftps option set tls-version` can be used to configure TLS version. By default, it is set to TLS v1.2. Recommended practice is to use TLS v1.2. But, for compatibility with FTP clients which use TLS v1.0/v1.1, TLS version can be set to TLS v1.0 or TLS v1.1.

Table 4. System inbound communication ports (continued)

Service	Protocol	Port	Port Configurable	Default	Description
SSH and SCP	TCP	22	Yes	Enabled	Port is used only if SSH is enabled. Run `adminaccess show` on the system to determine if it is enabled. SCP is enabled as default.
Telnet	TCP	23	No	Disabled	Port is used only if Telnet is enabled. Run `adminaccess show` on the system to determine if it is enabled.
HTTP	TCP	80	Yes	Disabled [a]	Port is used only if HTTP is enabled. Run `adminaccess show` on the system to determine if it is enabled.
DD Boost and NFS (portmapper)	TCP	111	No	Enabled	Used to assign a random port for the mountd service DD Boost and NFS use. Mountd service port can be statically assigned and can be started with the `nfs option set mountd-port` command.
NTP	UDP	123	No	Disabled	1. Port is used only if NTP is enabled on the system. Run `ntp status` to determine if it is enabled. 2. Used by the system to synchronize to a time server.
SNMP	TCP/UDP	161	No	Disabled	Port is used only if SNMP is enabled. Run `snmp status` to determine if it is enabled.
HTTPS	TCP	443	Yes	Enabled	Port is used only if HTTPS is enabled. Run `adminaccess show` on the system to determine if it is enabled.
CIFS (Microsoft-DS)	TCP	445	No	Enabled	Main port that is used by CIFS for data transfer.
DD Boost/NFS	TCP	2049	Yes	Enabled	Main port that is used by NFS. Run the `nfs option show` command on the system to determine the current NFS server port.
NFS v3/NFS v4	TCP	2049	Yes	Enabled	Main port that is used by NFS service. Run `nfs status` to determine if NFS v3 or NFS v4 service is enabled. Run `nfs option show nfs3-port` or `nfs option show nfs4-port` on system to determine the current port that is listening.
Replication	TCP	2051	Yes	Enabled	Port is used only if replication is configured on the system. Run `replication show config` to determine if it is configured. This port can be modified using the `replication modify` command.
NFS (mountd)	TCP/UDP	2052	Yes	Enabled	This can be changed through the `nfs option` command. The command can only be run by a Support Engineer. Contact Support if you need to change the port.

Table 4. System inbound communication ports (continued)

Service	Protocol	Port	Port Configurable	Default	Description
DDMC Port	TCP	3009	No	Enabled	This port is used only if the system is managed by the DDMC. It is not configurable.

a. Automatically redirects to HTTPS.

Table 5. System outbound communication ports

Service	Protocol	Port	Port Configurable	Default	Description
SMTP	TCP	25	No	Disabled	Used by the system to send email autosupports and alerts.
SNMP	UDP	162	Yes	Disabled	Used by the system to send SNMP traps to SNMP host. Use `snmp show trap-hosts` to see destination hosts and `snmp status` to display service status.
Syslog	UDP	514	No	Disabled	Used by the system to send syslog messages, if enabled. Use `log host show` to display destination hosts and service status.
RMCP	UDP	623	Closed	Disabled	Remotely access BMC through IPMI

To reach a system behind a firewall, you must enable the ports defined above.

Use the net filter functionality to disable all ports that are not used.

Table 6. Ports for Active Directory

Port	Protocol	Port configurable	Description
53	TCP/UDP	Open	DNS (if AD is also the DNS)
88	TCP/UDP	Open	Kerberos
139	TCP	Open	Netbios/Netlogon
389	TCP/UDP	Open	LDAP
445[1]	TCP/UDP	No	User authentication and other communication with AD
3268	TCP	Open	Global Catalog Queries

[1] Enabled by default on system and disabled on DDMC.

Network routing management

Routes determine the path taken to transfer data to and from the local host (the Data Domain or PowerProtect system) to another network or host.

DD OS does not generate or respond to RIP, EGRP/EIGRP, or BGP network routing management protocols in any form or fashion – DD OS cannot perform any IP packet routing or forwarding tasks. The only routing implemented on Data Domain or PowerProtect systems is based upon the internal route table, where the administrator may define which physical interface [interface group] to use to address a specific network or subnet. In addition, when multiple interfaces have the same subnet which will normally allow multiple interfaces to be used for packets going to the specific subnet, the appliance uses source-based routing. This defines that outbound network packets which matches the subnet of multiple interfaces will only be routed over the physical interface from which they originated from.

Time synchronization with external source

To configure time synchronization with an external source, see "Working with Time and Date Settings," "Data Domain System Clock," "Synchronizing from a Windows Domain Controller," and "Synchronize from an NTP Server" in the *DD OS Administration Guide*.

Cloud tier network security recommendations

To verify the identity of a cloud provider before backing up data from a Data Domain or PowerProtect system, the cloud providers have a host certificate issued by a certificate authority (CA). Import the CA certificate and any applicable certificate revocation lists (CRLs) before backing up any data to the cloud.

The following table shows the recommended settings for securely connecting to cloud tier storage.

Table 7. Cloud tier network security recommendations

Firewall port requirements[a]	• For ECS configuration, the system must be configured to allow traffic from ports 9020 and 9021. If a load balancer is configured on ECS, port rules have to be configured accordingly. • For Alibaba Cloud, AWS, and Google cloud providers, communication is on port 443 and 80.
OpenSSL cipher suites	• Ciphers - ECDHE-RSA-AES256-SHA384, AES256-GCM-SHA384 • TLS Version: 1.2
IP address range filtering	• Hostnames for Alibaba cloud provider to be resolved: ○ oss.aliyuncs.com ○ oss-us-west-1.aliyuncs.com ○ oss-us-east-1.aliyuncs.com ○ oss-ap-southeast-1.aliyuncs.com ○ oss-ap-southeast-2.aliyuncs.com ○ oss-ap-southeast-3.aliyuncs.com ○ oss-ap-southeast-5.aliyuncs.com ○ oss-ap-northeast-1.aliyuncs.com ○ oss-ap-south-1.aliyuncs.com ○ oss-eu-central-1.aliyuncs.com ○ oss-me-east-1.aliyuncs.com ○ oss-cn-hangzhou.aliyuncs.com ○ oss-cn-shanghai.aliyuncs.com ○ oss-cn-qingdao.aliyuncs.com ○ oss-cn-beijing.aliyuncs.com ○ oss-cn-zhangjiakou.aliyuncs.com ○ oss-cn-huhehaote.aliyuncs.com ○ oss-cn-shenzhen.aliyuncs.com ○ oss-cn-hongkong.aliyuncs.com • Hostnames for AWS cloud provider to be resolved: ○ s3.amazonaws.com ○ s3-us-west-1.amazonaws.com ○ s3-us-west-2.amazonaws.com ○ s3-eu-west-2.amazonaws.com ○ s3-eu-west-1.amazonaws.com ○ s3-ap-northeast-1.amazonaws.com ○ s3-ap-northeast-2.amazonaws.com ○ s3-ap-south.amazonaws.com ○ s3-ap-southeast-1.amazonaws.com ○ s3-ap-southeast-2.amazonaws.com ○ s3-sa-east-1.amazonaws.com ○ s3-eu-central-1.amazonaws.com

Table 7. Cloud tier network security recommendations (continued)

	• Hostname for Google Cloud: ○ storage.googleapis.com
Proxy settings	• A self signed/CA-signed certificate of proxy has to be imported using `adminaccess certificate import ca application cloud`. • If there are any existing proxy settings that reject data above a certain size, those settings must be changed to allow object size up to 4.5 MB.
Supported protocols	• HTTP • HTTPS

a. By default, ports 9020 and 9021 are not able to receive incoming network traffic. They must be enabled to receive incoming network traffic to use DD Cloud Tier.

For enhanced security, the Cloud Tier feature uses:

- Signature Version 2 for Alibaba Cloud and Google Cloud requests.
- Signature Version 4 for all AWS requests. AWS V4 signing is enabled by default.

Certificates for cloud providers

Before you can add cloud units for Alibaba Cloud, Amazon Web Services S3 (AWS), Azure, Elastic Cloud Storage (ECS), and Google Cloud Platform (GPC), you must import certificate authority (CA) certificates.

NOTE: The CLI to import the certificates for cloud providers is `adminaccess certificate import ca application cloud`.

Data Domain and PowerProtect use secure transport in all its communications with the public cloud providers and verifies the identity of the cloud provider. Each cloud provider has a host certificate that identifies the cloud provider and is issued by a CA.

As part of setting up the Cloud Tier, you must import the cloud provider's root CA certificate and any applicable certificate revocation lists (CRLs) on the system. This step must be performed before adding any cloud profiles for this cloud provider.

NOTE: Certificate auto-import is implemented if proxy is not involved. Refer to *DD OS Administration Guide* for more information.

Alibaba Cloud

1. Download the GlobalSign Root R1 certificate from https://support.globalsign.com/customer/portal/articles/1426602-globalsign-root-certificates.
2. Convert the downloaded certificate to a PEM-encoded format. The OpenSSL command for this conversion is: `openssl x509 -inform der -in <root_cert.crt> -out <root_cert.pem>`.
3. Import the certificate to the system.

AWS and Azure

1. Download root CA certificates from https://www.digicert.com/digicert-root-certificates.htm.
2. Convert the downloaded certificate to a PEM-encoded format. The OpenSSL command for this conversion is: `openssl x509 -inform der -in <root_cert.crt> -out <root_cert.pem>`.
3. Import the CA certificate to the system.

Elastic Cloud Storage (ECS)

ECS is a private cloud provider and resides within the data center, and it gives you the choice of either configuring the transport over HTTP or HTTPS.

If using HTTPS (secure transport), on the system, you must import the CA certificate from the load balancer front-ending the ECS nodes.

Google Cloud Platform (GCP)

1. Download the GlobalSign Root R1 certificate from https://support.globalsign.com/customer/portal/articles/1426602-globalsign-root-certificates.
2. Convert the downloaded certificate to a PEM-encoded format. The OpenSSL command for this conversion is: `openssl x509 -inform der -in <root_cert.crt> -out <root_cert.pem>`.
3. Import the certificate to the system.

The *DD OS Administration Guide* provides more details.

Cloud user credential

Alibaba Cloud, AWS S3, and Google Cloud have minimum permission requirements.

Alibaba Cloud

The Alibaba Cloud user credentials must have permissions to create and delete buckets and to add, modify, and delete files within the buckets they create. AliyunOSSFullAccess is preferred, but the following are the minimum requirements:

- ListBuckets
- GetBucket
- PutBucket
- DeleteBucket
- GetObject
- PutObject
- DeleteObject

By default, the bucket access permission would be set as "private" so it can only be accessed with AK authentication. Alibaba Cloud provides 3 types of AK(AccessKeyId and an AccessKeySecret) for authentication:

- Cloud account AccessKeys
- RAM (Resource Access Management) account AccessKeys
- STS (Security Token Service) account AccessKeys

NOTE: Data Domain and PowerProtect do not currently support STS account AccessKeys. Use Cloud account or RAM AK for authentication.

In accordance with the legal requirements of the People's Republic of China, account real-name registration must be completed in order to store data in OSS in the Mainland China region.

AWS S3

AWS S3 provides a way to restrict access rights to a specific bucket and IP address(es). It is recommended that the bucket policy restricts access rights to only that specific bucket. The read/write rights should only be allowed by the DDVE writing to the specific bucket.

NOTE: The AWS user credentials must have permissions to create and delete buckets and to add, modify, and delete files within the buckets they create. S3FullAccess is preferred, but the following are the minimum requirements:

- CreateBucket
- ListBucket
- DeleteBucket
- ListAllMyBuckets
- GetObject
- PutObject
- DeleteObject

Google Cloud

Google Cloud user credentials must have permissions to create and delete buckets and to add, modify, and delete files within the buckets they create. These are the minimum requirements:

- ListBucket
- PutBucket
- GetBucket
- DeleteBucket
- GetObject
- PutObject
- DeleteObject

DDVE in Cloud

The object store bucket (or "container" in Azure) that is created for a particular DDVE must not be shared with any other appliance or application. Sharing the bucket (or container) with other application or other DDVE could cause data loss and/or corruption.

For more information, see the applicable *DDVE Installation and Administration Guide*.

Network security

DDVE in cloud solution is a backend service. DDVE must be deployed in a private subnet and must not be exposed using public IP address. Most of the public IP address spaces are under continuous attacks by hackers.

Appropriate security groups network access lists shall be configured to enable only intended traffic to DDVE. Open only the required ports. A complete list of DDVE ports and their usage can be found in the applicable *DDVE Installation and Administration Guide*.

DDVE for kernel-based virtual machine considerations

Here are security recommendations for DDVE running on Kernel-based Virtual Machine (KVM).

- Do not provide access to non-admin users for the DDVE deployed and related files or storage on the host.
- The DDVE clock and the hypervisor host clocks must be in sync with each other to ensure that the time stamps match. To achieve this, configure the same NTP server on both the hypervisor and the DDVE. Alternatively, if NTP is not used on DDVE, then disable NTP on DDVE, and reboot so that it can sync its clock with the hypervisor host.

Secure multi-tenancy security

DD OS provides multiple security enhancements to enhance security for tenant administrators and tenant users.

Unique tenant-unit hostnames

A hostname that is configured for a tenant-unit cannot resolve to an IP address associated with another tenant-unit.

Data access isolation

Data access through the local IP addresses that are registered to a tenant-unit is restricted to the storage resources associated with that tenant unit.

The following constraints apply to data access isolation:

- The local IP address for data access must exist on the system.
- Existing IP addresses cannot be shared by multiple tenant-units.

- IP ranges are not supported.
- DHCP-assigned IP addresses are not supported.

Network firewall

The system can restrict access from specific remote IP addresses to provide those clients with access to specific tenant-unit IP addresses.

The following constraints apply to the network firewall:

- Remote data-access IP addresses cannot be shared between multiple tenants.
- Tenant exclusion checks are not performed for subnets or IP ranges.

Unique default gateways

The system can route data from different tenants through different routers or gateways, with separate default gateways that are configured for each tenant-unit, and the tenant-unit IP addresses mapped to the gateways for their associated tenant-unit.

The following constraints apply to unique default gateways:

- Targeted default gateways, which are assigned to a specific interface, are supported with secure multi-tenancy (SMT).
- Static, added, or DHCP gateways are not supported with SMT.
- A single default gateway cannot be shared between multiple tenants.
- Unique gateways that are assigned to a tenant cannot be used by non-SMT entities on the system.

There are no restrictions to the address used by the gateway.

Data security settings

Data security settings (including data encryption) enable controls that prevent data permanently stored by the product from being disclosed in an unauthorized manner.

NOTE: For more information about data encryption, see the Data Encryption section in this guide and the *DD OS Administration Guide*.

Dell EMC DD Retention Lock software

DD Retention Lock software provides immutable file locking and secure data retention capabilities for customers to meet both corporate governance and compliance standards, such as SEC 17a-4(f). DD Retention Lock provides the capability for administrators to apply retention policies at an individual file level. This software enables customers to use their existing systems for backup and archive data. DD Retention Lock ensures that archive data is retained long-term with data integrity and secure data retention.

DD Retention Lock Governance edition and DD Retention Lock Compliance edition can coexist on the same system. DD Retention Lock software is compatible with industry-standard, NAS-based (CIFS, NFS) Write-Once-Read-Many (WORM) protocols and is qualified with leading archive applications such as EMC SourceOne, EMC DiskXtender, and Veritas Enterprise Vault.

For Retention Lock Compliance, additional configuration needs to be done for setting and managing iDRAC users. See the *DD OS Administration Guide* for more details.

NOTE: The DD Compliance mode is not supported for DDVE.

Dual sign-on requirement

When DD Retention Lock Compliance is enabled, additional administrative security is provided in the form of “dual” sign-on. This requirement involves a sign-on by the system administrator and a sign-on by a second authorized authority (the “Security Officer”). The dual sign-on mechanism of the DD Retention Lock Compliance edition acts as a safeguard against any actions that could potentially compromise the integrity of locked files before the expiration of the retention period.

Secure system clock

DD Retention Lock Compliance implements an internal security clock to prevent malicious tampering with the system clock. The security clock closely monitors and records the system clock. If there is an accumulated two-week skew within a year between the security clock and the system clock, the file system is disabled and can be resumed only by a security officer.

On Retention Lock Compliant DD systems, system time can be modified only within certain restrictions set by date-change-limit and date-change-frequency. See the *DD OS Administration Guide* for mode details on setting system clock and NTP configuration.

Data integrity

- The DD OS Data Invulnerability Architecture™ protects against data loss from hardware and software failures.
- When writing to disk, the DD OS creates and stores checksums and self-describing metadata for all data received. After writing the data to disk, the DD OS then recomputes and verifies the checksums and metadata.
- After a backup completes, a validation process examines what was written to disk and verifies that all file segments are logically correct within the file system and that the data is identical before and after writing to disk.
- In the background, the online verification operation continuously checks that data on the disks is correct and unchanged since the earlier validation process.
- Storage in most systems is set up in a double-parity RAID 6 configuration (two parity drives). Also, most configurations include a hot spare in each enclosure, except in certain low-end series systems, which have eight or fewer disks. Each parity stripe has block checksums to ensure that data is correct. Checksums are constantly used during the online verification operation and while data is read from the system. With double parity, the system can fix simultaneous errors on as many as two disks.
- To keep data synchronized during a hardware or power failure, the system uses NVRAM (non-volatile RAM) to track outstanding I/O operations. An NVRAM card with fully charged batteries (the typical state) can retain data for hours, which is determined by the hardware in use.
- When reading data back on a restore operation, the DD OS uses multiple layers of consistency checks to verify that restored data is correct.

Data Domain and PowerProtect systems support SNMP V2C and/or SNMP V3. SNMP V3 provides a greater degree of security than V2C by replacing cleartext community strings as a means of authentication with user-based authentication using MD5, SHA1, or SHA-256. Also, SNMP V3 user authentication packets can be encrypted and their integrity that is verified with either DES or AES.

Multiple layers of data verification are performed by the DD OS file system on data that is received from backup applications to ensure that data is written correctly to the system disks. This process ensures that the data can be retrieved without error. The DD OS is purpose-built for data protection, and it is architecturally designed for data invulnerability. There are four critical areas of focus, described in the following sections: end-to-end verification, data erasure, system sanitization, and data encryption.

End-to-End verification

End-to-end checks protect all file system data and metadata.

As data comes into the system, a strong checksum is computed. The data is deduplicated and stored in the file system. After all data is flushed to disk, it is read back, and re-checksummed. The checksums are compared to verify that both the data and the file system metadata are stored correctly.

Data erasure

The `filesys destroy` command deletes all data in the file system. For more information on commands, see the *DD OS Command Reference Guide*.

NOTE: The Data Domain and PowerProtect data erasure is not compliant with DoD requirements. For DoD compliance, service Model Number: PS- BAS-DDDE is available.

System sanitization

System sanitization was designed to remove all traces of deleted files and restore the system to the previous state.

The primary use of the `sanitize` command is to resolve Classified Message Incidents (CMIs) that occur when classified data is copied inadvertently onto a non-secure system. System sanitization is typically required in government installations. Sanitization is not supported with SSD cache tier. Use the `storage remove` and `storage add` commands to remove the logical to physical mapping. This action ensures that physical pages not to return previous written data. However, the previously written data may still be on SSD.

For more information, see the *DD OS Administration Guide*.

Data encryption

There are three types of encryption offered with Data Domain and PowerProtect systems.

They are:

- Encryption of data at rest via the DD Encryption software option,
- Encryption of data in flight via DD Replicator software, which is used for replicating data between sites over the WAN, and
- Encryption of data in flight via DD Boost software, using TLS.

Encryption of data at rest

Encryption of data at rest protects user data in the situation where a Data Domain or PowerProtect system is lost or stolen and eliminates accidental exposure if a failed drive requires replacement. When the file system is intentionally locked, an intruder who circumvents network security controls and gains access to the system is unable to read the file system without the proper administrative control, passphrase, and cryptographic key. DD Encryption software is transparent to the backup or archive application.

DD Encryption provides inline encryption, which means as data is being ingested, the stream is deduplicated, compressed, and encrypted using an encryption key before being written to the RAID group. DD Encryption software uses RSA BSAFE libraries, which are FIPS 140-2 validated.

By default, the Embedded Key Manager (EKM) is in effect unless you configure KeySecure from Safenet Inc/Gemalto Keysecure or Data Security Manager (DSM) from Thales/Vormetric Key Management Interoperability Protocol (KMIP) key manager. External CA and Host certificates are required to set up KMIP-compliant key managers. You can request these certificates from third-party certificate authorities, or create them using appropriate OpenSSL utility. If encryption is enabled on Cloud Tier, only EKM is supported.

One of two cipher modes, Cipher Block Chaining mode (CBC) or Galois/Counter mode (GCM), can be selected to best fit security and performance requirements. The system also uses a user-defined passphrase to encrypt that key before it is stored in multiple locations on disk. The system encryption key cannot be changed and is not, in any way, accessible to a user. Without the passphrase, the file system cannot be unlocked, thus data is not accessible.

External key managers only supports AES-256.

For more information, see the *DD OS Administration Guide*.

Export encryption keys

Encryption keys are exported by running the `filesys encryption keys export` command. This applies to keys in both the active, cloud tier, and the retention tiers when cloud tier storage or DD Extended Retention is enabled. All encryption keys in the file system are exported to a file that can recover encryption keys in the system if required. The key file is passphrase encrypted, and you are prompted for a passphrase. To protect the key file, you may type a new passphrase that differs from the system passphrase. To perform this task, the *admin* or *limited-admin* role is required.

1. Run this command when a new key is created or when a change of state occurs to any of the existing keys.
2. Send the exported file using FTP for storage in a secure location, accessible to authorized users only.

NOTE: Lost or forgotten passphrases cannot be recovered.

Working with External Key Manager

Supported external key managers are Safenet Inc/Gemalto Keysecure and Data Security Manager (DSM) from Thales/ Vormetric.

External key managers are using Key Management Interoperability Protocol (KMIP) and centrally manages encryption keys in a single, centralized platform.

- Keys are pre-created on the Key Manager.
- External key manager cannot be enabled on systems that have encryption that is enabled on one or more cloud units.

Encryption of data in flight

Encryption of data in flight encrypts data being transferred via DD Replicator software between two DD systems. It uses OpenSSL AES 256-bit encryption to encapsulate the replicated data over the wire. The encryption encapsulation layer is immediately removed as soon as it lands on the destination system. Data within the payload can also be encrypted via DD encryption software.

Encryption of data in flight via NFS

NFSv3 and NFSv4 support krb5i and krb5p for integrity and privacy, respectively. However, there are performance penalties for encryption.

Encryption of data in flight through DD Boost

The DD Boost protocol can be used with or without certificates for authentication and encryption of data. The use of certificates was introduced to offer a more secure data transport capability.

In-flight encryption enables applications to encrypt in-flight backup or restore data over LAN from the system. When configured, the client can use TLS to encrypt the session between the client and the system. If TLS with certificates is used, then the specific suites that are used are DHE-RSA-AES128-GCM-SHA256 and DHE-RSA-AES256-GCM-SHA384 for medium and high encryption, respectively. If anonymous TLS is used to encrypt the session, then either ADH-AES256-GCM-SHA384, for the HIGH encryption option, or ADH-AES128-GCM-SHA256, for the MEDIUM encryption option, is used.

Secure Remote Services

Secure Remote Services is an IP-based automated connect home and remote support solution and creates both a unified architecture and a common point of access for remote support activities that are performed on the product. The Secure Remote Services IP Solution does the following:

- Provides continuous monitoring, diagnosis, and repair of minor hardware issues.
- Uses the most advanced encryption, authentication, audit, and authorization for ultra-high security remote support.
- Addresses compliance with corporate and governmental regulations by providing logs of all access events.
- Provides easy integration and configuration with the storage management network and firewalls.
- Provides maximum information infrastructure protection. IP-based sessions enable fast information transfer and resolution.
- Consolidates remote support for the information with the Secure Remote Services Gateway Client.
- Provides remote access to the disaster recovery site and makes recovery from unplanned events seamless.
- Protects information in motion or at rest. AES 256 encryption during information transfer protects the information.
- Reduces costs and data center clutter and accelerates time to resolution. The elimination of modem/phone line costs translates to lower costs.

NOTE: Secure Remote Services are not FIPS-compliant.

NOTE: Use of FTP or unsecure email while connecting to Secure Remote Services Gateway could be a security risk.

Secure Remote Services technical documentation is available on the online support site.

Security alert system settings

You can monitor system operation with a variety of DD System Manager tools: reporting tools that automatically send emails containing status and alerts, log files that contain a record of important system events, and SNMP monitoring using third party SNMP managers.

Automatic logging and reporting tools that provide system status to Dell EMC Support and designated email recipients are important in monitoring system operation. Their setup and use are described in this chapter.

Alerts are also sent as SNMP traps. See the *DD OS MIB Quick Reference* for the full list of traps.

For more information on handling alerts, see the *DD OS Administration Guide*.

Other security considerations

The section below describes additional steps you can take to increase your system's security.

Securing data in flight

Data can be vulnerable to man-in-the-middle (MITM) attacks when the attacker can impersonate an endpoint.

Replication

Data Domain and PowerProtect systems use self-signed certificates to build mutual trust between another system for secure data replication. It supports two different secure configurations using certificate that is one-way and two-way authentication.

DD OS supports one-way and two-way authentication between the replication source and destination to provide additional security for replication operations.

DD Boost

To avoid MITM attacks when an application is accessing the system, two way authentication which provides mutual verification must be done. Methods for doing two way authentication include certificates and Kerberos. DD Boost also supports two way authentication using pre-shared keys (PSK), which does not require certificates. Various applications may support one or more methods of two way authentication depending on the application and the protocol (such as DD Boost). For example, Avamar supports two-way authentication using certificates.

FIPS configuration

The DD file system, SMS, Apache HTTP service, LDAP client, and SSH Daemon use FIPS 140-2 compliant algorithms when FIPS is enabled. For instructions on how to enable FIPS mode, see the *DD OS Administration Guide*.

To enable FIPS compliance mode, run the following command: `system fips-mode enable`.

NOTE: Enabling or disabling FIPS compliance mode results in a system reboot and interrupts any ongoing backup or replication activities.

NOTE: Enabling FIPS mode invalidates all local users passwords. The passwords for sysadmin and one of the security officers are forced to change during enabling FIPS mode. The other local users require sysadmin to change their passwords for them by running `user change password`.

NOTE: All backup application using DD local users must restart the backups using new DD local user passwords. This is applicable for all protocols.

DD OS uses FIPS certified libraries including Dell OpenSSL Cryptographic Library, BSafe, Crypto J, Cert-J, and SSL-K.

- Dell OpenSSL Cryptographic Library v2.5
- EMC Crypto-C Micro Edition 4.1.4 cryptographic module

To disable FIPS compliance mode, run the following command: `system fips-mode disable`.

Table 8. Quick reference on Services vs FIPS compliant after FIPS is enabled on system

Service	Support FIPS	Configuration note
SSH	Yes	Compliant by enable FIPS
HTTPS	Yes	Compliant by enable FIPS
Telnet	No	Disabled by default; do not enable for FIPS
FTP/FTPS	No	Disabled by default; do not enable for FIPS
SMS	Yes	Compliant by enable FIPS
Data Encryption	Yes	Compliant by enable FIPS
Data Replication	Yes	Use Two-way authentication
NIS	Yes	Use SHA512 for user password hashing
LDAP	Yes	Use TLS authentication
SNMP	Yes	Use SNMPV3
DD Boost	Yes	DD Boost Client must be version 7.3 and higher
Active Directory	No	Not FIPS compliant
CIFS	No	Agnostic to FIPS mode setting
NFS	No	Not FIPS-compliant
Secure Remote Services	No	Disabled by default

SSH ciphers, MACs, and key exchange algorithms

When FIPS is enabled:

- Only FIPS 140-2 approved SSH ciphers and MACs can be set. User roles admin and limited-admin can set the ciphers and MACs, which can be configured by using the following command: `adminaccess ssh option set ciphers`
- The cipher list, MAC list, and KEX (key exchange algorithms) list in SSHD configuration file sets to a default list of FIPS-compliant ciphers, MACs, and KEXs. The old settings are lost.

When FIPS compliance mode is disabled, the cipher list, MAC list, and KEX (key exchange algorithms) list in SSHD configuration file sets to the system default list of ciphers, MACs and KEXs. The old settings are lost.

The following ciphers are supported on systems or DDVE running DD OS with FIPS enabled:

Table 9. Ciphers, MACs, and key exchange algorithms

Ciphers	• aes128-ctr • aes192-ctr • aes256-ctr
MAC	• hmac-sha2-256-etm@openssh.com • hmac-sha2-512-etm@openssh.com • hmac-sha2-256 • hmac-sha2-512
key exchange algorithms (KEXs)	• ecdh-sha2-nistp256 • ecdh-sha2-nistp384 • ecdh-sha2-nistp521 • diffie-hellman-group16-sha512 • diffie-hellman-group18-sha512 • diffie-hellman-group14-sha256

The cipher list can always be changed by running the `adminaccess ssh options set ciphers` command. When FIPS is enabled, users can only configure SSH service to use FIPS complaint SSH ciphers. If non-FIPS compliant ciphers are used, user would see an error.

The MAC list can always be changed by running the `adminaccess ssh options set macs` command. When FIPS is enabled, users can only configure SSH service to use FIPS complaint SSH macs. If non-FIPS compliant macs are used, user would see an error.

HTTPS

HTTPS Apache service uses the same list of cipher as SMS.

Data at rest encryption

If Data At Rest Encryption is enabled, then it is FIPS-compliant by default.

Replication control path and DDMC management communications

When FIPS compliance mode is enabled, only FIPS-compliant strong ciphers are used.

Replication is FIPS-compliant when it is enabled with two-way authentication.

If FIPS mode is enabled on the destination DD system, then Replication will not be allowed from DD systems running DD OS versions prior to DD OS 7.0.

The default cipher list is:

```
ALL:!ADH:!EXPORT56:!EXPORT40:+HIGH:!MEDIUM:!LOW:!SSLv2:!SSLv3:!DES-CBC3- SHA:
+EXP@STRENGTH
```

The client must use one of the following cipher suites:

- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- AES256-SHA256
- AES128-GCM-SHA256
- AES128-SHA256

The cipher list can be configured with the `adminaccess option set cipher-list` command.

NIS

If FIPS mode is enabled, ensure that the NIS server is configured using SHA512 for user password hashing. This applies to the existing NIS users and new users that are added to the NIS server. If NIS server is already configured, the previously supported NIS users may not be able to log in. All user passwords must be rehashed using SHA512.

LDAP

When FIPS is enabled, the LDAP client that runs on a system or DDVE must use TLS.

```
# authentication ldap ssl enable method start_tls
```

Otherwise, enabling FIPS compliance mode fails.

On a fresh install and upgrade, LDAP SSL ciphers are not explicitly set.

When FIPS compliance mode is enabled, the LDAP SSL ciphers are set to the following:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- AES256-GCM-SHA384

- AES256-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES128-SHA256
- AES128-GCM-SHA256
- AES128-SHA256

The configured cipher-list should be:

```
ECDHE-RSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-SHA384:DHE-RSA-AES256-GCM-SHA384:DHE-RSA-
AES256-SHA256:AES256-GCM-SHA384:AES256-SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-RSA-
AES128-SHA256:DHE-RSA-AES128-GCM-SHA256:DHE-RSA-AES128-SHA256:AES128-GCM-SHA256:AES128-
SHA256
```

When FIPS is disabled, it is set to `""`, an empty string.

SNMP

If the SNMP service is not required, disable the SNMP service.

If the SNMP service is required and enabled, the following is a list of the SNMP configurations that are needed before enabling FIPS mode.

- SNMP must be configured with SNMP V3.
- SNMP user authentication-protocol must be configured as SHA256.
- SNMP user privacy-protocol must be configured as AES.

SNMP v2/SNMP v1 protocols do not implement cryptographic security, and only SNMP v3 should be used when the system has FIPS enabled.

FIPS mode on the operating system running a DD Boost client

FIPS mode can be enabled on the operating system running an application that uses the DD Boost client to connect to a DD system, without the knowledge of the application and without enabling FIPS mode on the DD system. In such a scenario, either of the following configuration must be made:

- The DD Boost client on that operating system must be version >=7.1.
- The password hash for users on all DD systems that this client connects to must be `sha512`. This can be changed using the `adminaccess option set password-hash sha512` CLI.

If FIPS mode is enabled on the operating system without either of the above configurations, all connections from this client to any DD system will fail.

DD Boost Client with FIPS mode enabled

When FIPS mode is enabled on the system, applications accessing the system using the DD Boost protocol should use version 7.3 of the DD Boost client libraries. This guarantees operations are FIPS-compliant and use FIPS-compliant algorithms. Sometimes, the application may cause the DD Boost client libraries to enter FIPS mode if the application is FIPS aware and has been updated to enter FIPS mode in the client library. In that case not only will FIPS-compliant algorithms be used but the implementations of those algorithms use FIPS certified libraries.

When FIPS mode is enabled, the passwords set on the system that is used by DD Boost to access the system must have hash SHA512 values. A user with a password with an MD5 hash will be unable to connect to a FIPS enabled system.

NOTE: The Boost client library an application uses must be version >=7.1 in order for the application to connect successfully to a DD system running a DD OS version >=7.1 with FIPS mode enabled. The DD Boost client library version that ships with an application is determined by the application provider. A list of all Boost clients that have connected to the DD system in the last 24 hours can be obtained from the `ddboost show connections` CLI. The `Plugin Version` column should be referred to in order to determine whether any client with a Boost plugin older than 7.1.x.x is currently connecting to this DD system. All such clients will fail to connect after FIPS mode is enabled on the DD system and must be

upgraded. Check with the application vendor to determine the DD Boost client library version a specific application version uses to see if the application can be used with a DD system with FIPS mode enabled.

Telnet

Telnet is not FIPS-compliant and is disabled by default.

FTP/FTPS

FTP/FTPS is not FIPS-compliant and is disabled by default.

Active Directory

Active Directory is not FIPS-compliant.

Active Directory continues to work when it is configured and when FIPS is enabled.

CIFS

CIFS server on DD OS is agnostic to FIPS mode setting. Even if the customer enables FIPS mode, CIFS continues to work in non-FIPS compliant mode.

To disable or stop CIFS from accepting any connections from the clients:`sysadmin@localhost# cifs disable`

NFS

NFS is not FIPS-compliant.

- NFS continues to work in a non-FIPS compliant mode.
- NFS can be disabled with the `nfs disable` command.

Secure Remote Services (formerly ESRS)

Secure Remote Services is a secure, two-way connection between Dell EMC products and Dell EMC Customer Support. Secure Remove Service is disabled by default and continues to work in non-FIPS compliant mode.

System hardening and best practices

The hardening process is twofold. Traditionally, customers that are looking to harden a system are doing so because they are either under mandate, or are practicing secure computing practices. These tables provide both the hardening procedures and the mitigation steps to comply with federal Defense Information Systems Agency (DISA) Security Technical Implementation Ulde (STIGs) on the device.

Table 10. Administrative access

Description	Hardening recommendation
Change default password.	Log in as sysadmin and run `# user change password` See the *DD OS Command Reference Ulde* "user change" section for more information.
Configure frequent password rotation according to the company's password policy.	Follow company password policy to set the default password aging policy. `# user password aging option set {[min-days-between-change <days>]`

Table 10. Administrative access (continued)

Description	Hardening recommendation

	`[max-days-between-change <days>]`
	`[warn-days-before-expire <days>]`
	`[disable-days-after-expire <days>]}`
	
	See the *DD OS Command Reference Gulde* "user password" section for more information.

Configure a strong password policy.	Set user password strength policy:
	
	`# user password strength set`
	`{[min-length <length>]`
	`[min-character-classes <num-classes>]`
	`[min-one-lowercase {enabled | disabled}]`
	`[min-one-uppercase {enabled | disabled}]`
	`[min-one-digit {enabled | disabled}]`
	`[min-one-special {enabled | disabled}]`
	`[max-three-repeat {enabled | disabled}]`
	`[passwords-remembered <0 - 24>]}`
	
	Password recommendations:
	• A minimum of nine characters
	• A minimum of one lowercase character
	• A minimum of one uppercase character
	• A minimum of one numeral
	• A minimum of one special character
	• No spaces

Enable security officer.	Add security officer role user, force password change, and enable Authorization Policy.
	
	Use `user add` command to add security officer as a security role user.
	
	`# user add <user>`
	`[uid <uid>]`
	`[role {admin | limited-admin | security |`
	`user | backup-operator | none}]`
	`[min-days-between-change <days>]`
	`[max-days-between-change <days>]`
	`[warn-days-before-expire <days>]`
	`[disable-days-after-expire <days>]`
	`[disable-date <date>]`
	`[force-password-change {yes | no}]`
	
	Set `force-password-change` to **yes** when adding the security officer account.
	
	Log in as security officer, and run `# authorization policy set security-officer enabled`

Use limited-admin for day-to-day operation instead of admin or sysadmin.	Add a limited-admin role user and set a password different to sysadmin/admin role users.
	
	`# user add <user>`
	`[uid <uid>]`
	`[role {admin | limited-admin | security |`
	`user | backup-operator | none}]`
	`[min-days-between-change <days>]`
	`[max-days-between-change <days>]`
	`[warn-days-before-expire <days>]`
	`[disable-days-after-expire <days>]`
	`[disable-date <date>]`
	`[force-password-change {yes | no}]`

Change the password of the security officer that is created by sysadmin.	Log in as security officer, and then run `# user change password`

Table 10. Administrative access (continued)

Description	Hardening recommendation

Use client list to restrict access only to required hosts.	For SSH:
	● Add an SSH host.
	`# adminaccess ssh add <host-list>`
	● Delete hosts from the SSH list.
	`# adminaccess ssh del <host-list>`
	For HTTP and HTTPS:
	● Add an HTTP/HTTPS host.
	`# adminaccess http add <host-list>`
	● Delete hosts from the HTTP/HTTPS list.
	`# adminaccess http del <host-list>`
	NOTE: Do not use a wildcard character enabling access for any user. Type individual IP addresses or client names instead.

Monitor syslog to watch user creation and other sensitive activities in the system.	● Configure and forward logs to syslog server. ● Monitor audit log and access log. See the *DD OS Command Reference Ulde* for more information. ○ `# log view access-info` ○ `# log view audit-info` ● Consider writing a script that runs the above commands several times a day and reports any suspicious activities. ● Pay close attention to sensitive and not often used commands that are related to user access management and network settings, including time setting. ● Monitor authentication and authorization failures in particular. ● Monitor all operations that require password. ● Monitor destruction operations and any failures and repeating attempts. ● Highly recommended is to write searches and dashboards to view log forwarded info. Also setup alerts rules on your log server.
Provide security officer credentials different from sysadmin.	Set different passwords for sysadmin, admin role users, and security officer.
No single person should know the sysadmin and security officer credentials.	It is recommended to have different persons as sysadmin and as security officer.
Use certificates issued by the customer's data center.	DD systems come with self-signed certificates. It is recommended to import the certificates from customer's data center. See Certificate management for more information.
Use `netfilter` to disable ports if not required.	For example, disable port 111 and 2049 if DD Boost is not in use.
Do not enable telnet.	Disable telnet by running `# adminaccess disable telnet`
Use FTPS and SCP, but not FTP.	FTP by default is disabled. Use FTPS and SCP, but not FTP.
Use SNMP v3 when SNMP is configured.	When SNMP is configured, enable SNMPv3. Ensure SNMPv1 and SNMPv2c are disabled.

Table 11. Encryption

Description	Hardening recommendation
Use external key manager for encryption.	See the DD Encryption section in the *DD OS Administration Gulde* for instructions on configuration. Additional information can be found in the Encryption for data at rest section of this Ulde for security best practices.
Use of encryption algorithm and key length	The recommendation is to use 256-bit keys and AES algorithm in GCM mode. See the "filesys encryption" section of the *DD OS Command Reference Ulde*.
Configure system passphrase.	Set and use a hardened system passphrase. The default minimum length requirement is 9 characters. Use `system passphrase option set min-length` to set higher length requirements. See the "system passphrase" section of *DD OS Command Reference Ulde* for more information.

Table 12. TLS for FTP

Description	Hardening recommendation
TLS-version	By default, FTPS will enable TLSv1.2 from DDOS 7.5. TLS versions TLSv1.0 and TLSv1.1 are disabled by default, if required please use tls-version configuration option provided to enable TLS versions TLSv1.0 and TLSv1.1.
Cipher-list	Default cipher-list supports only TLSv1.2. To enable TLSv1.0 and TLSv1.1, change cipher-list accordingly.

Table 13. Replication

Description	Hardening recommendation
Use encryption and two-way authentication.	Configure two-way authentication when adding a replication pair. `# replication add source <source> destination <destination> [low-bw-optim {enabled | disabled}] [encryption {enabled [authentication-mode {one-way | two-way | anonymous}] | disabled}] [propagate-retention-lock {enabled | disabled}] [ipversion {ipv4 | ipv6}] [max-repl-streams <n>] [destination-tenant-unit <tenant-unit>]`

Table 14. DD Boost

Description	Hardening recommendation
Set global-authentication-mode to two-way-password and enabled encryption.	By default the global authentication mode is set to none, and the encryption is disabled. The configurations ensure only DD Boost clients with at least two-way-password authentication support, those using DD Boost 3.3 or later, can attach and data is encrypted on the wire. `# ddboost option set global-authentication-mode two-way-password global-encryption-strength <high/medium>`
Set password hash support to SHA512 <support client version greater than 3.5>	By default the password hash is set to MD5. Modifying this to SHA512 prevents DD Boost clients unable to support the SHA512 from attaching.

Table 14. DD Boost (continued)

Description	Hardening recommendation
	`# adminaccess option set password-hash {md5 | sha512}`

Configure DD Boost users with a role of none.	Create a none role user and associates it to be a DD Boost user.
	`# user add <user> role none`
	`# ddboost user assign <user>`

Limit the assignment of a DD Boost user to a single storage unit.	Do not assign the same DD Boost user to multiple DD Boost storage-units. This limits the number of DD Boost clients that share the same DD Boost user credentials.
Use client list to limit access.	`# ddboost clients add client-list [encryption-strength {none | medium | high} authentication-mode {one-way | two-way | twoway-password | anonymous | kerberos}]` **NOTE:** During configuration, do not use a wildcard character enabling access for any user. Type individual IP addresses or client names instead.
Enable encryption with two-way authentication for managed file replication.	Use authentication-mode two-way. `# ddboost file-replication option set encryption enabled authentication-mode two-way`
Configure NFS port to use something other than 2049 to prevent NFSv3 client access.	`# nfs option set nfs3-port <new port number>` `# nfs option set nfs4-port <new port number>`
Use Kerberos for BoostFS.	Clients connecting to the DD system using BoostFS are encouraged to use Kerberos support only if FIPS is not an option. DD system Active Directory support must be configured. To configure BoostFS client's to use Kerberos, see the platform specific *DD BoostFS Configuration Ulde*
Use Avamar default security settings for DD Boost connectivity if using Avamar.	Avamar by default use two-way TLS certificates, encryption, and token access for clients. It is recommended keeping the default.
If DD Boost or NFS is not in use, use netfilter option to disable portmapper port 111.	`# net filter add operation block protocol tcp ports 111` `# net filter add operation block protocol udp ports 111`

Table 15. NFS

Description	Hardening recommendation
Configure Kerberos with encryption.	Ensures that data on the wire is encrypted. `# nfs export create <export name> path <path> option sec=krb5p`
Specify list of hosts who can access export.	Delete NFS clients from an export `# nfs add <path> <client-list> [ ( <option-list> ) ]`

Table 15. NFS (continued)

Description	Hardening recommendation
	Delete NFS clients from an export. `# nfs del <path> <client-list>` **NOTE:** When configuring, do not use a wildcard character enabling access for any user. Type individual IP addresses or client names instead.
Not using `no_root_squash`	Verify using the following command: `# nfs export show list` Should verify `no_root_squash` is not configured for any exports.

Table 16. VTL/vDisk

Description	Hardening recommendations
Use default options.	Existing default options are considered best practices.

The following table contains DISA STIG/SRG rules with their corresponding hardening steps. These recommendations can be used to comply with DISA STIG standards for our device type.

Table 17. DISA STIG standards

Description	Hardening recommendation
Enable FIPS 140-2 approved encryption.	DD supports use of only FIPS 140-2 approved ciphers for secured connections. DD recommends using UI or CLI to enable FIPS mode: • UI: **Administration** > **Setting** > **FIPS mode** • CLI: `system fips-mode enable` See the FIPS configuration section for more details.
The application server must limit the number of concurrent sessions to an organization-defined number for all accounts and account types.	DD recommends UI or CLI hardening: • UI: **Administration** > **Access** > **More Tasks** > **Change Login Options** (to set active login to 100) • CLI: `adminaccess option set login-max-active 100`

The network device must be configured to enforce the limit of three consecutive invalid logs in attempts, after which time it must block any login attempt for 15 minutes.	DD recommends use of UI or CLI to configure:
	• UI: **Administration** > **Access** > **More Tasks** > **Change value on Maximum login Attempts as 3, Unlock timeout as 900 sec**
	• CLI:
	  ○ `adminaccess option set login-max-attempts 3`
	  ○ `adminaccess option set login-unlock-timeout 900`

The application server must automatically terminate a user session after organization-defined conditions or trigger events requiring a session disconnect. The system must be configured so that all network connections that are associated with a communication session are terminated at the end of the session or after 10 minutes of inactivity from the user at a command prompt, except to fulfill documented and validated mission requirements.	DD supports terminating connections at the end of the session and support session termination after configured time of inactivity. There is a CLI to specify the inactivity period. SSH connection is still alive but any request from client is rejected. A session clean-up process is running and clean-up and terminates sessions that are no longer valid. DD recommends the following for UI or CLI hardening: • UI: **Administration** > **Access** > **Check on HTTPS** > **Configure** > **ADVANCE** and set timeout value as 600 sec. Repeat the same for SSH by clicking **SSH** in **Services**.

Table 17. DISA STIG standards (continued)

Description	Hardening recommendation

	• CLI:
	  ○ SSH: `adminaccess ssh option set session-timeout 600`
	  ○ https: `adminaccess web option set session-timeout 600`

Various password aging requirements	DD recommends CLI `user password aging option`. By default the password policy is relaxed to be backward compatible. The customer can use UI or CLIs to modify the password configuration so it is more restrictive and meets the aging requirements. • UI: **Administration** > **Access** > **More Tasks** > **Change Login Options** **NOTE:** Per user option can be set through **Administration** > **Access** > **Local Users** > **Modify** > **Advanced** • CLI: `user password aging`
Various Passwords strength requirements	DD supports comprehensive password policy and recommends using CLI or UI to harden the password. Customers can set or modify account password policy characteristics and complexity to whatever is wanted within the application code. This feature mitigates those findings. • UI: **Administration** > **Access** > **More Tasks** > **Change Login Options** • CLI: `user password strength set`
Operating system must, for networked systems, synchronize clocks with a server that is synchronized to one of the redundant United States Naval Observatory (USNO) time servers, a time server designated for the appropriate DoD network (NIPRNet/SIPRNet), and/or the Global Positioning System (GPS).	DD recommends using UI or CLI to configure NTP server. • UI: **Administration** > **Settings** > **MORE TASKS** > **Configure Time Settings** Enter NTP server info by clicking the **+** sign. • CLI: `ntp add timeserver <server-name> ntp enable`
The Apache web server must be configured to use a specified IP address and port.	DD supports different HTTPS port and limiting of certain interface instead of default of all interfaces for HTTPS connections. DD recommends using `adminaccess` and `netfilter` CLI command to harden: • `adminaccess web option set https-port <port>` • `net filter add operation allow protocol tcp ports <port> interfaces <IP_address>` **NOTE:** IP address must be an active interface reported by `ifconfig` command.

The application server must uniquely identify all network-connected endpoint devices before establishing any connection.
The Apache web server must restrict inbound connections from nonsecure zones.
	To restrict inbound connections, DD recommends configuring allowed host in HTTPS and SSH connections using UI or CLI command.
	• UI: **Administration** > **Access** > **ADMINISTRATOR ACCESS** > **select HTTPS/SSH** > **CONFIGURE** > **GENERAL** and click the **+** (Add) sign.
	• CLI:
	  ○ `adminaccess http add <host_list>`
	  ○ `adminaccess ssh add <host-list>`

Notifications when reaching audit log storage capacity	Email alert can be sent when audit log storage space reaches 80% and 100% threshold. DD recommends use of UI or CLI to configure the system to "Send Alert Notification Emails."

Table 17. DISA STIG standards (continued)

Description	Hardening recommendation

	• UI: **Health** > **Alerts** > **NOTIFICATION** > **ADD**(Groups on file system Class with WARNING and CRITICAL and Subscriber CONFIGURE (Add email addresses and Groups)
	• CLI:
	  ○ `alerts notify-list create <group name warning> class filesystem severity warning`
	  ○ `alerts notify-list add <group name warning> emails <email>`
	  ○ `alerts notify-list create <group name critical> class filesystem severity critical`
	  ○ `alerts notify-list add <group name critical> emails <email>`

Enabling Audit Log Forwarding:	DD supports syslog forwarding and recommends using CLI to set up connection to a remote syslog server. • `log host add <Remote_syslog_Server>` • `log host enable`
Using Authentication Server for authenticating users before granting administrative access.	DD supports multiple name servers protocols such as LDAP, NIS, and AD. DD recommends using OpenLDAP with FIPS enabled. DD manages only local accounts. DD recommends using UI or CLI to configure LDAP. • UI: **Administration** > **Access** > **Authentication** • CLI: Authentication LDAP commands
The network device must authenticate network management SNMP endpoints before establishing a local, remote, or network connection using bi-directional authentication that is cryptographically based.	DD supports SNMPV3 that is FIPS-compliant. DD recommends using UI or CLI to configure SNMPV3. • UI: **Administration** > **Settings** > **SNMP** • CLI: SNMP commands
The application server must accept Personal Identity Verification (PIV) credentials to access the management interface.	DD supports using of DoD issued CAC/PIV card at client browser to login using UI. This is a multi-factor login using certificate of CAC/PIV card. DD recommends UI or CLI command to configure MFA and set up OpenLDAP for user authorization. General Procedure: • Configure OpenLDAP Import CA certificate to DD. • Import DoD CA to DD • Create local users (if LDAP authentication is not used). • Disable password-based login For more information about configuration steps, see the *DD OS Administration UIde* and *DD OS Command Reference UIde*.
The application server, for PKI-based authentication, must implement a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information over the network.	DD supports CRL on MFA with issuing CA revoking CAC certificate by importing CRL cert to DD. DD recommends using CLI to import CRL certificate. • CLI: `adminaccess certificate cert-revoke-list import application login-auth`
The Apache web server must be configured to immediately disconnect or disable remote access to the hosted applications.	DD recommends disabling HTTPS service to terminate all active sessions by UI or CLI. • UI: **Administration** > **Access** > **Administrator Access** > **HTTPS** > **CONFIGURE** (clear HTTPS and save). • CLI: `adminaccess disable https`

Table 17. DISA STIG standards (continued)

Description	Hardening recommendation
The Red Hat Enterprise Linux operating system must not allow a noncertificate trusted host SSH log in to the system.	DD supports SSH connection using ssh keys instead of password-based login. If password-based login is disabled, UI login using password is also disabled. DD recommends using CLI to import key certificate and disable password-based SSH login. ● CLI: ○ `adminaccess add ssh-keys user <user_name>` ○ `adminaccess option set password-auth disable` **NOTE:** Sysadmin account must have ssh key imported first to disable password-based login.
Use a FIPS 140-2 approved cryptographic hashing algorithm.	The system must use a FIPS 140-2 approved cryptographic hashing algorithm for generating account password hashes. Systems must employ cryptographic hashes for passwords using the SHA-2 family of algorithms or FIPS 140-2 approved successors. The use of unapproved algorithms may result in weak password hashes more vulnerable to compromise. **NOTE:** The *DD OS Command Reference Ulde* describes how to use the `adminaccess option set passwordhash {md5 | sha512}` command to set the FIPS 140-2-approved cryptographic hashing on the system. Changing the hash algorithm does not change the hash value for any existing passwords. Any existing passwords that were hashed with md5 will still have md5 hash values after changing the password-hash algorithm to sha512. Those passwords must be reset so that a new sha512 hash value is computed.
Remove telnet-server package.	Telnet can be removed. Run `adminaccess uninstall telnet` to remove the telnet package from the DD system. **NOTE:** If telnet is removed, it cannot be added back to the system.
Audit log forwarding to remote syslog server	DD supports forwarding of local audit log to syslog server. ● CLI ○ log host add <Remote_syslog_IP> ○ log host enable **NOTE:** Corresponding configuration to accept DD's syslog at Remote Syslog server is required.
User's consent to Notice and Consent Banner	DD can be configured to prompt for user consent prior to login to DD's UI interface. ● UI: **Administration** > **LOGIN BANNER** > **CONFIGURE** ● CLI: `system option set login-banner /ddr/var/releases/<banner_file>` ● `Where <banner_file> is uploaded to DD's /ddr/var/releases as text file`

3

Secure Maintenance

This chapter includes:

Topics:

Security patch management

Your contracted service provider is responsible for installing the latest security patches. Contact Dell EMC Support for additional information.

4

Physical Security Controls

This chapter includes:

Topics:

Physical controls

Physical security controls enable the protection of resources against unauthorized physical access and physical tampering.

The DS60 has a disk drive locking mechanism that prevents the removal of a disk drive without the appropriate tool, which is a T10 Torx screwdriver. The bezel on the ES30, ES40, FS15, and FS25 has a lock and key that prevents access to the drives.

DD3300, DD6300, DD6800, DD6900, DD9300, DD9400, and DD9900 systems have ES30-style bezels.

DD9800 systems have a lock and a key, which prevents access to the drives.

For more information, see the related expansion shelf and hardware guide or disk FRU replacement documentation for the specific product.

Baseboard management controller and basic input/output system recommendations

This list contains the recommended baseboard management controller (BMC) and basic input/output system (BIOS) security practices.

- Always flash the latest BMC and BIOS images as they are released even if the release notes do not explicitly state a security fix.
- Use the Administrator Password in BIOS setup.
- Use strong passwords for IPMI user accounts and BIOS administrator password.
- Set up an isolated network for manageability and never expose that network to the internet.
- If using onboard NICs for manageability is required, configure VLANs to isolate it from the host network.

General USB security best practices

1. Prohibit booting from USB (or any device other than the hard disks) in BIOS.
2. Disable the USB ports completely in BIOS (if possible).
3. Setting a password in BIOS.

The following sections provide the general operations for disabling USB and password setup in BIOS.

Disabling USB in BIOS

For DD6900, DD9400, & DD9900, the process is:

1. After entering BIOS setup by pressing F2 after reboot, browse to **System BIOS Settings** > **Integrated Devices**

2. Set **User Accessible USB Ports** to **All Ports Off**.

For DD9800, the process is:

1. Browse to **IntelRCSetup** > **PCH Configuration** > **PCH Devices** > **USB Configuration**.
2. Set **USB Controller 0 Enable** to **Disabled**.

   NOTE: Another available option is to set **USB Ports Per-port Disable** to **Enabled**, and then disable each port respectively.

For DD6300, DD6800, and DD9300, the process is:

1. Browse to **IntelRCSetup** > **PCH Configuration** > **USB Configuration** > **USB Ports**.
2. Set **Per-port** from**Disable** to **Enable**.
3. Disable each port as needed.

Setting BIOS password

1. Browse to **Security** > **Administrator Password**.
2. Type the password to be set in **Create New Password**.
3. **Confirm New Password** window.
4. After reset, system will ask you for password if you want to enter BIOS setup menu.

Clearing BIOS password

1. Browse to **Security** > **Administrator Password**.
2. Type the current password in **Enter Current Password** window.
3. Without any input in **Create New Password** window, press **Enter** from keyboard.

Securing Integrated Dell Remote Access Controller 9 (iDRAC)

iDRAC features

iDRAC provides user with the following features:

- Monitors server health
- Remotely power on, off, or cycle system
- Provides view of system inventory

Because iDRAC is independent from the DD OS, users can access a powered on system even if DD OS is not running.

iDRAC physical connection

iDRAC can be accessed through the dedicated iDRAC port in the back of the system. By default, this port is enabled with IP address 192.168.0.120. If this port is not used, users can choose to disable iDRAC port.

iDRAC services and ports

iDRAC supports many services that are separated from DD OS services. Configure these services appropriately to correctly secure the system.

The following table shows the available iDRAC services, ports, and their default setting.

Table 18. DD3300 iDRAC services and ports

Services	Ports	Description	Default Setting
Local Configuration	Not applicable	Disable access to iDRAC configuration (from the host system) using local RACADM and iDRAC Setting utility	Disabled
Web Server *	80 & 443	iDRAC web interface	Enabled
SSH *	22	Access iDRAC through SSH	Enabled
Telnet	23	Access iDRAC through Telnet	Disabled
Remote RACADM *	Not applicable	Remotely access iDRAC	Enabled
SNMP Agent	161	Enable support for SNMP queries in iDRAC	Disabled
Automated System Recovery Agent	Not applicable	Enable Last System Crash Screen	Disabled
Redfish *	Not applicable	Redfish RESTful API	Enabled
VNC Server	5901	VNC Server on iDRAC	Disabled
Virtual Console	5900	Virtual Console of iDRAC	Disabled

* These services must be enabled for system's functionality.

Table 19. DD6900, DD9400, and DD9900 iDRAC services and ports

Services	Ports	Description	Default Setting
Local Configuration	Not applicable	Disable access to iDRAC configuration (from the host system) using local RACADM and iDRAC Setting utility	Disabled
Web Server *	80 & 443	iDRAC web interface	Enabled
SSH *	22	Access iDRAC through SSH	Enabled
Telnet	23	Access iDRAC through Telnet	Disabled
Remote RACADM *	Not applicable	Remotely access iDRAC	Enabled
SNMP Agent	161	Enable support for SNMP queries in iDRAC.	Disabled
Automated System Recovery Agent	Not applicable	Enable Last System Crash Screen	Disabled
Redfish *	Not applicable	Redfish RESTful API	Enabled
VNC Server	5901	VNC Server on iDRAC	Disabled
RMCP	623	Remotely access BMC through IPMI	Disabled

* These services must be enabled for system's functionality.

To configure iDRAC services, see *Integrated Dell Remote Access Controller 9 User Guide*.

If an attempt is made through iDRAC access to unlock the virtual console, the following warning is displayed.

Figure 3. DD OS iDRAC banner

See the Knowledge Base article "Security Considerations and Best Practices for iDRAC et SNMP monitoring" for more information.

iDRAC accounts

iDRAC has the following password-protected default accounts:

- Root: The default password is the system serial number. User can use this account to monitor system hardware. User is recommended to change the default password.
- Reserved: The account is disabled by default. It is reserved for system internal functionality. User must not use, edit, or remove this account.
- PTAdmin: The account is enabled by default. It is reserved for system internal functionality. User must not use, edit, or remove this account.

For detailed instruction how to configure account, see *Integrated Dell Remote Access Controller 9 User Guide*.

Serial over LAN best practices

- Access the console through the iDRAC dedicated port.
- Create an iDRAC "operator" account with only **Login** and **Access Virtual Console** boxes checked.
- Limit the time that the console is open. It is recommended to not change the default setting for Serial Console Idle Timeout (300 seconds).
- Restrict which remote client/IP can SSH to iDRAC. The recommendation is to limit access from core switch such as ACL or VLAN tagging.

iDRAC hardening

The following table has information relating to additional iDRAC hardening.

Table 20. iDRAC

Description	Hardening recommendation
Restrict the number of Administrator (admin-role) accounts.	Create a restricted number of admin role accounts. The admin-role account has the "Configure Users" privilege so it is important to give this to a trusted person. Instructions on how to configure an admin-role account are as follows: 1. Log in to iDRAC using the root account. 2. Go to **iDRAC Settings** > **Users** > **Local Users**. 3. Click **Add**. 4. Fill out required fields. The password should be different from the DD OS sysadmin password. 5. Select **Administrator** for User Role. Confirm that all 9 privileges are selected. 6. Select **Administrator** for LAN Privilege Level. 7. Select **Administrator** for Serial Port Privilege Level.

Table 20. iDRAC (continued)

Description	Hardening recommendation
	8. Select **Enabled** for Serial Over LAN. 9. Click **Save**.
Disable default root account.	By default, the root account of iDRAC is enabled and the password is the PSNT of the system. It is insecure to keep the root account. The recommendation is to disable it. **CAUTION: The root account should only be disabled after another admin-role account is created to avoid losing system management ability.** 1. Log in to iDRAC using another admin-role account. 2. Go to **iDRAC Settings** > **Users** > **Local Users** 3. Select the root account, and click **Disable**.
Do not change PTAdmin account.	PTAdmin is required for system functionality. Do not modify this account.
Have different credentials for iDRAC users	Set different password for different iDRAC accounts
Password of admin-role account should be different from DD OS sysadmin and security officer password.	Set different password than the DD OS sysadmin and security officer accounts for the admin-role user.
Enable two-factor authentication for iDRAC login	To add an additional layer of security when logging in, it is recommended to turn on 2-Factor Authentication. 1. Configure SMTP a. Log in to iDRAC. Go to **Configuration** > **System Settings** > **Alert Configuration** > **SMTP (Email) Configuration** > **SMTP (Email) Server Settings**. b. Fill out required fields, and click **Apply**. 2. Enable 2-FA for an iDRAC account a. Log in to iDRAC. Go to **iDRAC Settings** > **Users** > **Local Users**. b. Select the wanted account, and click **Edit**. c. Select **Enabled** for Simple 2-FA. d. Click **Test Connection**. e. If successful, click **Save**.
Give "Control and Configure System" and "Access Virtual Console" privileges only to trusted persons.	When adding additional accounts in iDRAC, only give "Control and Configure System" and "Access Virtual Console" privileges to trusted persons.
Disable IPMI	IPMI is by default that is disabled. It is recommended to not enable it.
Limit access to iDRAC Virtual Console	It is recommended that the Virtual Console is disabled. If Virtual Console is to be enabled, account that has the privilege "Access Virtual Console" should only be given to trusted persons.

Příloha č. 6

Obecná pravidla pro dodavatele v oblasti bezpečnosti IT

1) Pokud jsou tato obecná pravidla v rozporu s ustanovením textu smlouvy nebo zadávací dokumentace nebo její jinou přílohou, má přednost ustanovení textu smlouvy nebo zadávací dokumentace nebo její jiná příloha.
2) Dodavatel je povinen zajistit, že jeho pracovníci či poddodavatelé a jejich pracovníci, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se u objednatele seznámí a které nejsou veřejně dostupné. Povinnost mlčenlivosti není časově omezena.
3) Dodavatel je rovněž povinen chránit informace, které nejsou veřejně dostupné, zejména předanou dokumentaci, před jejich prozrazením a/nebo zpřístupněním neoprávněným osobám a dále použít získané informace výhradně pro účely plnění smlouvy s ČNB.
4) Dodavatel nemá vzdálený přístup k systémům a do počítačové sítě ČNB.
5) Pracovníci dodavatele, kteří budou samostatně přistupovat k informačním systémům a systémovému prostředí ČNB, se před nebo při prvním přístupu musí seznámit s bezpečnostními požadavky a svými povinnostmi vyplývajícími z vnitřních předpisů ČNB.
6) Dodavatel a jeho pracovníci nejsou oprávněni:
   a) obcházet bezpečnostní mechanizmy prostředků výpočetní techniky;
   b) sdělovat své přístupové údaje k systémům ČNB;
   c) sdílet přístup k systémům ČNB (umožnit jinému pracovat pod uživatelovým oprávněním);
   d) provádět akce požadované třetí osobou (instalace softwaru, návštěva webových stránek apod.) bez ověření oprávněnosti požadavku.
7) Dodavatel a jeho pracovníci jsou povinni:
   a) okamžitě nahlásit sekci informatiky ČNB, pokud identifikují možnost obejití bezpečnostních mechanizmů prostředků výpočetní techniky. To neplatí pro dodavatele, jejichž předmět smlouvy obsahuje tuto činnost;
   b) při opuštění pracovní stanice stanici uzamknout (např. vytažením multifukčního průkazu ze stanice) nebo se odhlásit, a ověřit, že k odhlášení/uzamčení opravdu došlo;
   c) bezpečně zlikvidovat nepotřebná výměnná média (např. CD/DVD, flash disk, paměťová karta) prostřednictvím služby HelpDesku ČNB;
   d) bez prodlení odebrat z tiskárny vytištěné dokumenty, popřípadě pro zajištění důvěrnosti použít zabezpečený tisk, pokud to nastavení tiskárny umožňuje;
   e) v případě detekce viru nebo podezření na přítomnost škodlivého kódu neprodleně kontaktovat HelpDesk ČNB a stanici kompletně prověřit antivirovým programem za případné spolupráce HelpDesku ČNB.
8) Pracovníci dodavatele nesmí:
   a) zaznamenávat heslo tak, aby mohlo být snadno identifikováno (týká se i zapisování do elektronických dokumentů, např. Notepad). Pro uchování je možné použít například bezpečné úložiště na čipové kartě uživatele (SmartNotes);

b) používat stejná hesla v systémech ČNB a pro přístup do dalších systémů a aplikací mimo ČNB (např. soukromá e-mailová schránka, Facebook, LinkedIn).

9) Pracovníci dodavatele nejsou oprávněni:

a) používat soukromou e-mailovou schránku pro činnosti související s plněním dle smlouvy, kromě výjimečné situace, která nesnese odkladu a při níž hrozí nebezpečí z prodlení v případě nedostupnosti nebo poruchy pracovního e-mailu;

b) nastavovat automatické přeposílání e-mailů z pracovní e-mailové adresy mimo systémové prostředí ČNB;

c) ukládat jiné než veřejné informace mimo úložiště pod správou ČNB nebo dodavatele (případně pod správou smluvně zajištěného partnera), zejména do cloudových služeb (např. uloz.to, leteckaposta.cz, Google Disk, Microsoft OneDrive a další).

10) Dodavatel a jeho pracovníci nejsou oprávněni:

a) nepovoleně používat, kopírovat a šířit software, jako např.:

i) instalovat nebo spouštět na počítačích ČNB soukromě pořízený software (včetně softwaru licencovaného na uživatele jako soukromou osobu);

ii) instalovat nebo spouštět na počítačích ČNB z internetu stažený software (včetně komerčního software, software typu shareware, freeware, public domain a software licencovaného modelem GPL – General Public Licence). To neplatí v případech, kdy předmět smlouvy obsahuje tuto činnost;

iii) instalovat či přenášet software ve vlastnictví ČNB na jiné počítače ČNB, na své soukromé počítače nebo na počítače třetích stran nebo pořizovat kopie softwaru instalovaného v počítači ČNB. To neplatí

(1) pro situace výslovně schválené a popsané v jiném vnitřním předpisu (např. vzdálený přístup ze zařízení, které není ve vlastnictví ČNB) a

(2) v případech, kdy předmět smlouvy obsahuje tuto činnost;

b) používat nebo poskytnout neoprávněně jiným uživatelům sériová čísla, licenční klíče, hardwarové klíče nebo jiné technické prostředky sloužící k zajištění ochrany nebo jednoznačné identifikaci vlastníka licence softwaru získané v ČNB;

c) bránit spouštění nástrojů sloužících pro automatizované kontroly nainstalovaného a spouštěného softwaru a provádět činnosti, které by vedly ke zkreslení získaných dat z těchto nástrojů.

Archivace elektronické pošty

1) Zpráva zaslaná tak, že alespoň jedním z adresátů zprávy je emailová adresa ...@cnb.cz, se ukládá současně s přijetím i do dlouhodobého archivního úložiště.

2) Veškeré zprávy odesílané z emailové adresy ...@cnb.cz se ukládají do dlouhodobého archivního úložiště současně s odesláním.

Kontrola přístupu na Internet

Z důvodu zvláštní povahy činnosti ČNB a z toho plynoucí povinnosti zajištění bezpečnosti informačních systémů ČNB, z nichž některé jsou součástí kritické informační infrastruktury

státu, jsou přístupy uživatelů na Internet ze sítě ČNB automaticky zaznamenávány na úrovni domén 2. řádu (tj. např. idnes.cz).

Příloha č. 7

Bezpečnostní požadavky ČNB

1. Zhotovitel odpovídá za to, že do objektů objednatele (dále jen „ČNB“) budou vstupovat nebo vjíždět pouze ti jeho pracovníci, kteří jsou jmenovitě uvedeni v písemném seznamu schváleném ČNB (dále jen „seznam“). Tato povinnost se vztahuje i na posádky vozidel zhotovitele vjíždějících do garáží ČNB za účelem složení a naložení nákladu. Seznam zhotovitel předloží ČNB nejpozději den před zahájením prací.
2. Seznam bude obsahovat tyto položky: jméno, příjmení a číslo průkazu totožnosti každého z pracovníků zhotovitele. Zhotovitel se zavazuje zajistit, aby všichni jeho pracovníci uvedení v seznamu byli ještě před předložením seznamu ČNB proškoleni o podmínkách zpracování osobních údajů a o právech subjektů údajů ve smyslu obecného nařízení o ochraně osobních údajů - Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (dále jen „GDPR“). Zhotovitel se zejména zavazuje, že všichni jeho pracovníci uvedení v seznamu budou nejpozději do okamžiku předložení seznamu ČNB poučeni:
   a) o tom, že zhotovitel předá jejich osobní údaje v rozsahu: jméno, příjmení a číslo průkazu totožnosti České národní bance, sídlem Na Příkopě 28, Praha 1 v rámci plnění této smlouvy, a to za účelem ochrany práv a oprávněných zájmů ČNB (zajištění evidence osob vstupujících do budovy ČNB z důvodu ochrany majetku a osob a správy přístupového systému ČNB);
   b) o veškerých právech subjektu údajů, která mohou uplatnit vůči zhotoviteli a ČNB, zejména o právu na přístup k osobním údajům, které jsou o nich zpracovávány, právu na námitku proti zpracování osobních údajů, právu požadovat nápravu situace, která je v rozporu s právními předpisy, a to zejména formou zastavení nakládání s osobními údaji, jejich opravou, doplněním či odstraněním, jakož i o právu podat stížnost k Úřadu pro ochranu osobních údajů.
3. Za poučení svých pracovníků ponese zhotovitel vůči ČNB následně odpovědnost. V případě nesplnění povinnosti podle bodu 2. nahradí zhotovitel újmu, která v souvislosti s uvedeným ČNB vznikne, a to včetně případné nemajetkové újmy vzniklé poškozením dobrého jména a dobré pověsti, újmy vzniklé v důsledku postihu pravomocně uloženého ČNB správním nebo jiným k tomu oprávněným orgánem veřejné moci a újmy vzniklé ČNB v důsledku úspěšného uplatnění práv pracovníků zhotovitele vůči ČNB.
4. Požadavky na případné doplňky a změny schváleného seznamu je nutno neprodleně oznámit ČNB. Případné doplňky a změny seznamu podléhají schválení ČNB. Osoby neschválené ČNB nemohou vstupovat do objektů ČNB, přičemž ČNB si vyhrazuje právo neuvádět důvody jejich neschválení.
5. Při příchodu do objektů ČNB pracovníci zhotovitele sdělí důvod vstupu, prokáží se osobním dokladem a podrobí se bezpečnostní kontrole. Osoby, které nejsou uvedeny v seznamu, nebudou do objektů ČNB vpuštěny.
6. Schválení pracovníci zhotovitele musí dbát pokynů bankovních policistů, které se týkají režimu vstupu, pohybu a vjezdu do objektu ČNB. Pracovníci zhotovitele budou do prostor ČNB vstupovat a v těchto prostorách se pohybovat v režimu návštěv, to znamená vždy pouze v doprovodu zaměstnance ČNB nebo zaměstnance referátu bankovní policie ČNB.
7. V případě mimořádné události se pracovníci zhotovitele musí řídit pokyny bankovních policistů nebo dozorujícího zaměstnance ČNB, a dále instrukcemi vyhlašovanými vnitřním

rozhlasem ČNB.

8. Pracovníci zhotovitele nesmí vnášet do prostor ČNB nebezpečné předměty, jako jsou střelné zbraně, výbušniny apod. O tom, co je či není nebezpečný předmět, rozhodují bankovní policisté v souladu s vnitřními předpisy ČNB.
9. ČNB si vyhrazuje právo nevpustit do objektů ČNB pracovníka zhotovitele, který je zjevně pod vlivem alkoholu, drog nebo jiné omamné látky.
10. Bez písemného povolení ČNB je zakázáno fotografování a pořizování videozáznamů z interiéru objektů ČNB.
11. Ve všech prostorech objektů ČNB je přísný zákaz kouření a používání otevřeného ohně. O povolení práce se zvýšeným požárním nebezpečím požádá zhotovitel písemnou formou vždy nejpozději jeden pracovní den před zahájením prací dozorujícího zaměstnance ČNB. Dále se pracovníci zhotovitele musí zdržet poškozování či odcizování majetku ČNB, a dále i jakéhokoli nevhodného chování vůči zaměstnancům a návštěvníkům ČNB.
12. Pracovníci zhotovitele uvedení v seznamu se musí před započetím výkonu práce v objektech ČNB seznámit, ve smyslu předpisů o požární ochraně, bezpečnosti a hygieně práce, se specifiky daných objektů ČNB (např. způsob vyhlášení požárního poplachu, určení ohlašovny požáru, seznámení s únikovými cestami, poplachovými směrnicemi, evakuačním plánem, umístěním věcných prostředků požární ochrany apod.). ČNB je oprávněna kdykoliv podrobit kontrole kterékoliv pracovníka zhotovitele uvedeného na seznamu ohledně dodržování těchto předpisů a ustanovení.

Příloha č. 8

Specifikace cen plnění

Položka	Cena v Kč bez DPH	Cena celkem v Kč bez DPH
1.dílčí plnění		
Realizační projekt	80000	80 000,00
Cena celkem za 1. dílčí plnění		**80 000,00**
2.dílčí plnění		
technické prostředky včetně instalace	4373832	4 373 832,00
programové prostředky včetně instalace	1200000	1 200 000,00
zaškolení zaměstnanců	24000	24 000,00
Cena celkem za 2. dílčí plnění		**5 597 832,00**
3.dílčí plnění		
realizační dokumentace a ostatní plnění v rámci 3. dílčího plnění zvlášť neuvedené	54000	54 000,00
Cena celkem za 3. dílčí plnění		**54 000,00**
Celková cena díla v Kč bez DPH		**5 731 832,00**
Technická podpora	Cena v Kč bez DPH služby za 1 měsíc	
Podpora technických prostředků po dobu trvání smlouvy	8000	
Podpora programových prostředků po dobu trvání smlouvy	8000	

Příloha č. 9

Významné součásti realizačního projektu

V závislosti na konkrétní použité technologii bude realizační projekt obsahovat zejména informace o:

- způsob zapojení dodávaných technických a programových prostředků do struktur objednatele (zejména SAN a LAN);
- logické konfiguraci prostředků (např. definice knihoven a drivů nebo konfigurace RAID Group apod.);
- systému vytváření 3. kopie zálohovaných dat;
- popis zabezpečení na všech úrovních proti neoprávněné modifikaci dat;
- systému implementace a přidělování drivů v DataProtector;
- postupu přechodu na další zařízení.

Příloha č. 10

Protokol o zkušebním provozu

Provedené testy

Test	Požadovaná hodnota	Výsledek	Poznámka*)
Parametry pro zálohování			
Kompatibilita s DataProtector	ano		
Kapacita (v každé lokalitě)	4000 TB		
Počet paralelních session	20		
Celkový výkon	2000 MB/s		
Přístupová doba k médiu	---		
Připojení drivů	FC/LAN		
Připojení drivů	identifikace		
Přenos dat mezi objekty	FC/LAN		
Dostupnost	24x7, upgrade mikrokódu a výměna komponent za provozu		
Uložení informací	Zachovány po výpadku napájení		
Provádění 3.kopie dat	Typ technologie		Pouze pro úplnost – formální doplnění
Provádění kopie dat-výkonnost	Bez ovlivnění prováděných záloh		Provádění kopií nesmí snižovat požadovanou výkonnost 200 MB/s
Provádění kopie dat-časová okna	Ovlivňování časových oken stávajících backupů		
Provádění kopie dat-aktualizace média DB	Zajištění aktualizace media DB		Jen v případě, že se replikace děje na jiné úrovni než DP
HDD (kontrola čitelnost stop/sektorů v době nižší aktivity)	Automatická kontrola čitelnost dat na HDD		Pouze doporučující požadavek a navíc jen v případě, že data budou na HDD
Zabezpečení (bude kontrolováno dle konkrétní vybrané technologie, zde uvedeny body jen rámcově)			
Povolené porty pro přístup z LAN	minimalizace		
Konfigurace managementu	Minimální možný přístup		
Účty a oprávnění	Minimalizace		
Zajištění proti modifikaci	Nelze modifikovat		
Zajištění proti smazání	Nelze smazat		
Obecné požadavky			
Kompatibilita se servery	ano		Formální kontrola
Kompatibilita s prostředím ČNB	ano		Formální kontrola

Deduplikace	Zajištění kontroly shodných řetězců		Formální kontrola
Komprese	Typ komprese (HW/SW), zajištění výkonu		Formální kontrola
Hmotnost	Max. 550 kg		Formální kontrola
Rozměry	Maximální výška 195 cm, 90 cm x 110 cm		Formální kontrola
Napájení	1-fázové, 230 V		Formální kontrola
Zátěž SAN	Není zbytečné zatížení pro vlastní režii		
Dohledový nástroj	Bezpečnostní kritéria, zasílání informací		
Konfigurační změny	bezpečnost		

*) Ve sloupci „poznámka“ je nyní uveden pouze komentář

Optimalizace:

Typ optimalizace	**Výsledek** *)
Zálohování	
Drive – výkon (nastavení parametrů v DP)	Kontrola řádného nastavení počtu a velikosti buffer atd.
Média – počet, typ, velikost, formát	Kontrola počtu médií, jejich typu (např. norewind), velikosti a formátu ve vztahu k nastavení drivů a ve vztahu k optimální rychlosti použití (zápis a čtení) médií
Média – umístění (jen v případě uložení na discích)	Kontrola rozložení médií na RAID groupách apod.
Celkový výkon	Kontrola rychlosti a optimálního rozložení v kontextu navržené technologie
Rozložení backup session/přidělování drivů	Kontrola, že celý systém funguje optimálně ve vztahu k nadefinovaným backup session, kopiím do druhé lokality a přidělování drivů

*) Ve sloupci „výsledek“ je nyní uveden pouze komentář

Příloha č. 11

Obsah realizační dokumentace

Realizační dokumentace systému zálohování obsahuje následující součásti:

1. Dokumentace skutečného stavu systému zálohování po implementaci technických a programových prostředků podle čl. I odst. 1 smlouvy, v níž bude zachycen popis konečného stavu a provozních postupů, zejména:
    - skutečný stav zapojení;
    - nastavení systému;
    - postupy při provozu;
    - nastavení komunikace ze zařízení.
2. Havarijní plány obsahující:
    - základní postupy při problémech spolupráce s DataProtector (např. vymontování pásky z drivu, přidání média, apod.);
    - popis postupu při běžných závadách, které nemají zásadní vliv na funkčnost knihovny (např. výměna disku, výměna SFP modulu apod.);
    - postupy při složitějších závadách, kdy zálohovací systém ztratí konektivitu s knihovnou nebo její částí (výpadky FC tras, výpadek celé knihovny, apod.).

Cílem této dokumentace není nahrazení dokumentace dodávané výrobcem, ale zejména popis specifik provozu v ČNB a zvýraznění nejčastějších postupů uvedených v dokumentaci výrobce