DECISION
SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO Ltda

Item 1 - DD6900

Brasília (Sede)
Setor Hoteleiro Sul - Quadra 06 - Conjunto 'A'
Bloco A - Sala 102 - Asa Sul - Brasília/DF
Cep: 70.322-915 - Tel: (61) 2045.0050

Salvador
Avenida Tancredo Neves, 620 - Salas 2910 e 2911
29º andar - Torre Empresarial do Ed. Mundo Plaza
Caminho das Árvores - Salvador/BA - Cep: 41.820-020
Tel: (71) 3585.7007

São Paulo
Rua Arizona, 1.422 - Conjunto 76 - Ed. Platinum
Building Berrini - Berrini - São Paulo/SP - Cep: 04.567-003
Tel: (11) 5583.0044

Número do artigo: 000186133 Imprimir

Ações de limpeza de unidade de disco rígido suportadas de Dell de limpeza de dados (NIST 800 88r1)

Resumo: Informações sobre comandos compatíveis com a limpeza de dados Dell.

Conteúdo do artigo

Sintomas

Nenhuma informação sobre o sintoma.

Causa

Nenhuma informação sobre a causa.

Resolução

Dell informações do comando de limpeza de dados

Em geral, os requisitos de limpeza que são colados abaixo são os requisitos de implementação do fabricante. Dell a remoção de dados emite os comandos na tabela abaixo do disco rígido.

O fabricante da unidade implementará o comportamento de limpeza para atender à especificação National Institute of Standards and Technology (NIST). O BIOS está emitindo apenas o comando, e não informando diretamente a unidade como executar o comando. O BIOS não controla o comportamento da unidade depois que os comandos de limpeza são emitidos para a unidade.

Dependendo da mídia, comandos diferentes são emitidos. O resultado será um descarte, ou um status claro, dependendo do tipo de mídia (unidade de disco rígido giratório ou da unidade de estado sólido (SSD)) (**tabela 1**).

Media	Comando	Digite NIST 800-88r1
Disco rígido ATA	Eliminação de segurança aprimorada	Exclusão
SSD ATA	Eliminação de segurança aprimorada	Desmarque
eMMC	Apagar/limpar	Exclusão
SSD PCIE M. 2	Eliminação de segurança aprimorada	Desmarque
NVMe PCIe SSD	Formato NVM (NVM de formato)	Exclusão

Tabela 1 -comandos de limpeza de dados do disco rígido

NIST diretriz de 800 88r1: NIST a publicação especial 800-88 – diretrizes para o saneamento de mídia o declara o seguinte:

Limpar, descartar e destruir são ações que podem ser executadas para limpar a mídia. As categorias de saneamento são definidas como:

- Clear aplica técnicas lógicas para limpar os dados em todos os locais de armazenamento que são endereçáveis pelo usuário. Para proteção contra técnicas simples de recuperação de dados não invasivas; Geralmente, são aplicados por meio dos comandos de leitura e gravação padrão para o dispositivo de armazenamento, por exemplo, por meio da regravação com um novo valor ou usando uma opção de menu para redefinir o dispositivo para o estado de fábrica (onde a regravação não é suportada).

- A remoção aplica técnicas físicas ou lógicas que colocam a recuperação de dados de destino inviável usando técnicas de laboratório de ponta a ponta.

- A destruição faz com que a recuperação de dados de destino seja inviável por meio de técnicas de laboratório de estado de arte e resulte na incapacidade subsequente de usar a mídia para armazenamento de dados.

Artigos relacionados:

- Número do artigo 000150908: Processos de remoção de dados para uma unidade de disco rígido de estado sólido

- Número do artigo 000146892: Dell Data Wipe

- Número do artigo 000134997: Usando a função de limpeza de dados do Dell BIOS para OptiPlex, Precision e sistemas Latitude criados após novembro de 2015

Voltar ao início

Propriedades do artigo

Data da última publicação

04 mai 2021

Versão

1

Tipo de artigo

Solution

Oracle Backup Solutions Program (BSP)

What is the Backup Solutions Program?

Many organizations rely on Oracle to provide solutions for very large or highly distributed mission critical systems. In addition to needing databases capable of handling large amounts of data and complex queries, these organizations also need robust backup and recovery technology. Recovery of data quickly and reliably is paramount should some aspect of the system fail. To address these needs, Oracle has created the Backup Solutions Program (BSP), a cooperative program designed to facilitate tighter integration between Oracle's backup products and those of third-party media management vendors. Together, Oracle and media management vendors provide robust, easy-to-use database backup and recovery solutions to customers with high-end requirements.

Backup Solutions Through Partnership

Oracle designed an architecture that allows Oracle backup products to manage the process of database backup and recovery, yet integrates with industry-leading tape storage management subsystems. The interface between Oracle's products and media management vendor products is keyed on an Oracle design specificatic
backup products to use third party media management s
from tape.

In this way, the robustness and expertise of both Oracle a
is leveraged: Oracle drives the database backups, and the
provides the mechanism for managing the storage and r

How to Become a Member

Becoming a member of BSP is the method with which third-party media management vendors receive the information, tools, and resources they require to develop the integration media management technology solutions for Oracle customers.

When using Oracle backup products, customers are able to choose from leading tape storage management systems provided by Backup Solutions Program member companies. Minimum requirement to become a BSP member or to maintain BSP membership is to be an active Oracle partner.

To receive more information on becoming a member, send an email to infobsp_us_grp@oracle.com.

Media Management Vendor Partners

Under the BSP, vendors are committed to integrating Recovery Manager (RMAN) with their media management software packages and provide first line technical support for the integrated backup and recovery solutions for Oracle RDBMS.

Following is the list of media management software vendors that have joined the Oracle Backup Solutions Program (BSP).

Company	Product	Contact	Email address	Contact Phone
Aishu	AnyBackup	Aaron Wang	aaron.wang@aishu.cn	+86-400-880-1569
Asigra Inc.	Asigra Cloud Backup	Eran Farajun	eran.farajun@asigra.com	416-736- 811 x1801
Chengdu Vinchin Technology Co., Ltd.	Vinchin Backup & Recovery	Luwen Zhang	luwen.zhang@vinchin.com	
CommVault Systems	QiNetix Galaxy B/R	Audrey DeNovio	adenovio@commvault.com	732-870-4651
Cohesity	Cohesity Appliance			
Druva	Phoenix		sales@druv	
eCloudTech	eCloud Data Backup	Penny Mao	contact@ecl	

Company	Product	Contact	Email address	Contact Phone
EMC	EMC Disk Library EMC Networker EMC Avamar EMC DD Boost for RMAN	Tom Papadakis Shailesh Manjrekar	tom.papadakis@emc.com shailesh.manjrekar@emc.com	905-315-4707 408-421-4214
HP	Data Protector		imhub@hp.com	US: 877-686-9637 EMEA: +08-70-013-0790
Hitachi Vantara	Ops Center Protector		GCC.Email.Requests@hitachivantara.com	1-800-446-0744
Information2	i2Backup	Chen Wang	marketing@info2soft.com	+86-400-6178-60
Quantum Corporation	DXi Backup Appliances	Steve Wright	steve.wright@quantum.com	(800) 677-6268
Infinidat	Infiniguard		info@infinidat.com	1-855-900-4634
Rubrik	Rubrik Cloud Data Management		oracle@rubrik.com	1-844-
Scutech Corporation	DBackup InfoSemper	James (Zijun) Wang	jzwang@scu	
Shanghai Suninfo Information Technology	ADM	Capricorn (Gang) Dang	dangg@sun	

Company	Product	Contact	Email address	Contact Phone
Symantec/Veritas	NetBackup Backup Exec			
Veeam	Backup & Replication		support@veeam.com	800-774-512

Número do artigo: 000003886

Imprimir

Data Domain: Noções básicas sobre a compactação do Data Domain

Resumo: As terminologias, vantagens e medidas são explicadas aqui para descrever os tipos de compactação usados, a terminologia e outros aspectos da compactação de um sistema Data Domain.

Conteúdo do artigo

Instruções

Noções básicas sobre a compactação do Data Domain

OBJETIVO

As técnicas de compactação envolvidas em um sistema Data Domain utilizam técnicas de última geração para reduzir o espaço físico exigido pelos dados dos clientes. Portanto, as tecnologias e as medições dos níveis de compactação são tópicos complexos. Este documento discute algumas terminologias, vantagens e medidas para explicar melhor os tipos de compactação usados, a terminologia e outros aspectos da compactação de um sistema Data Domain.

APLICA-SE A

- Todos os sistemas Data Domain

SOLUÇÃO

1. Introdução

Última atualização: 21 de junho de 2012

Compactação é uma tecnologia de redução de dados que visa a armazenar um conjunto de dados usando menos espaço físico. Nos sistemas Data Domain (DDOS), nós fazemos uma *desduplicação* e uma *compactação local* para compactar os dados do usuário. A desduplicação, ou deduplicação, é usada para identificar segmentos de dados redundantes e armazenar apenas segmentos de dados exclusivos. A compactação local compacta ainda mais os segmentos de dados exclusivos com determinados algoritmos de compactação, como lz, gzfast, gz etc. A compactação geral de dados do usuário no DDOS é o esforço conjunto entre a desduplicação e a compactação local. O DDOS usa a "*taxa de compactação*" para medir a eficácia da compactação de dados. Geralmente, ela é a proporção entre o tamanho total dos dados do usuário e o tamanho total dos dados compactados ou o tamanho do espaço físico usado.

O file system do Data Domain é um file system de desduplicação "estruturado por logs". Um file system estruturado por logs só acrescenta dados ao sistema, e a exclusão por si só não pode liberar espaço físico. Esses file systems dependem da coleta de lixo para recuperar o espaço que não é mais necessário. Combinadas, as características do file system estruturado por logs e da tecnologia de desduplicação dificultam o claro entendimento de todos os aspectos da compactação do DDOS.

Nós podemos medir muitos aspectos sobre a compactação. Neste documento, discutiremos os detalhes passo a passo para ajudar a entender a compactação do DDOS. Primeiramente, explicaremos o efeito geral da compactação do sistema, que nos informa a compactação *realista* realizada em um sistema Data Domain: o volume de dados do usuário, a quantidade de espaço físico consumido e a proporção entre eles. Neste documento, essa proporção é chamada de "taxa de compactação efetiva do sistema". O DDOS realiza a desduplicação em linha e monitora as estatísticas dos segmentos originais de dados do usuário, os segmentos de dados exclusivos pós-desduplicação e o efeito da compactação local sobre os segmentos de dados exclusivos. Essas estatísticas de compactação em linha são usadas para medir o efeito da compactação em linha. Observe que as estatísticas de compactação em linha podem ser medidas em cada gravação. Além disso, o DDOS monitora as estatísticas em diferentes níveis: arquivos, MTrees e o sistema inteiro.

O conteúdo deste documento pode ser aplicado a todas as versões do DDOS lançadas até a publicação deste documento, o DDOS 5.3. Não há garantias de que todo o conteúdo seja preciso para versões futuras. Nas versões anteriores à 5.0, o sistema como um todo tem apenas uma MTree e o termo MTree não é explicitamente acionado.

2. Compactação: Efeito geral no sistema

O efeito geral da compactação em todo o sistema é medido pela *taxa de compactação efetiva do sistema*, que é a proporção entre o tamanho dos dados do usuário e o tamanho do espaço físico usado. Ele é relatado pelo comando "filesys show compression" (FSC) da

CLI (as informações correspondentes também estão disponíveis na GUI). Um exemplo de resultado do FSC é exibido abaixo.
From: 2012-06-07 13:00 To: 2012-06-14 13:00 Pre-Comp Post-Comp Global-Comp Local-Comp Total-Comp (GiB) (GiB) Factor Factor Factor (Reduction %) ———— —— —— —— —— ———Currently Used: 614656.0 135747.2 - - 4.5x (77.9)Written:* Last 7 days 6914.1 1393.7 3.4x 1.5x 5.0x (79.8) Last 24 hrs 1067.7 218.7 3.4x 1.5x 4.9x (79.5) ———— —— —— —— —— ———* Does not include the effects of pre-comp file deletes/truncates since the last cleaning on 2011/03/19 16:09:04. Key: Pre-Comp = Data written before compression Post-Comp = Storage used after compression Global-Comp Factor = Pre-Comp / (Size after de-dupe) Local-Comp Factor = (Size after de-dupe) / Post-Comp Total-Comp Factor = Pre-Comp / Post-Comp Reduction % = ((Pre-Comp - Post-Comp) / Pre-Comp) * 100
A taxa de compactação efetiva do sistema é informada na linha 1 da seção de resultados da saída da CLI. A linha é destacada em envelope. O tamanho total dos dados do usuário é identificado como "Pre-Comp". O espaço físico total consumido (por dados e metadados) é exibido como "Post-Comp".
Observe que os números "Pre-Comp" e "Post-Comp" são lidos no tempo de execução. O FSC sincroniza implicitamente o sistema inteiro e, então, consulta os dois números. Esses dois números são medidos da mesma forma que `"filesys show space"`.
Taxa de compactação efetiva do sistema = Pre-Comp/Post-Comp
O restante do resultado do FSC descreve as estatísticas de compactação em linha, que nós discutiremos posteriormente.
Há várias operações que podem afetar a taxa de compactação efetiva do sistema:

- **Cópia rápida**. Quando uma operação de cópia rápida é feita a partir de um arquivo do namespace ativo (não a partir de snapshots), ela é uma desduplicação perfeita, pois não é necessário ter espaço físico extra para o arquivo de destino. Uma cópia rápida permite aumentar o tamanho dos dados do usuário sem consumir espaço físico adicional. Isso aumentará a taxa de compactação efetiva do sistema. Quando muitas cópias rápidas são feitas, a taxa de compactação efetiva do sistema pode se tornar artificialmente alta.
- **Sintético virtual**. Os backups sintéticos virtuais tendem a mostrar uma alta taxa de compactação efetiva do sistema. Isso ocorre porque a opção sintética virtual faz backups completos lógicos, mas só transfere dados alterados/novos para os sistemas Data Domain. O impacto da opção sintética virtual sobre a taxa de compactação efetiva do sistema é um pouco semelhante ao efeito da cópia rápida.
- **Substituições**. As substituições consomem mais espaço físico, mas não aumentam o tamanho lógico do conjunto de dados. Assim, elas reduzem a taxa de compactação efetiva do sistema.
- **Armazenar arquivos fragmentados**. Os arquivos fragmentados contêm grandes "furos" que são contabilizados no tamanho lógico, mas não consomem espaço físico devido à compactação. Como resultado, eles podem fazer com que a taxa de compactação efetiva do sistema pareça alta.
- **Armazenar arquivos pequenos**. O DDOS adiciona uma sobrecarga de quase 1 KB a cada arquivo para determinados metadados internos. Quando um sistema armazena um número significativo de arquivos muito pequenos (tamanhos inferiores a 1 quilobyte ou em quilobytes de um dígito), a sobrecarga dos metadados diminuirá a taxa de compactação efetiva.
- **Armazenar arquivos pré-compactados/pré-criptografados**. A compactação e a criptografia podem amplificar significativamente o nível de alteração de dados e reduzir a possibilidade de desduplicação. Geralmente, esses arquivos não podem ser desduplicados satisfatoriamente e reduzir a taxa de compactação efetiva do sistema.
- **Exclusões**. As exclusões reduzem o tamanho lógico do sistema, mas o sistema só recupera o espaço não utilizado correspondente quando a coleta de lixo é executada. Um grande número de arquivos excluídos deixará a taxa de compactação baixa até que a GC seja executada.
- **Coleta de lixo (GC)**. A GC recupera o espaço consumido pelos segmentos de dados que não são mais referidos por nenhum arquivo. Se muitos arquivos foram excluídos recentemente, a GC poderá aumentar a taxa de compactação do sistema reduzindo o espaço físico consumido.
- **Captura agressiva de snapshots**. Quando capturamos um snapshot de uma MTree, nós não alteramos o tamanho lógico do conjunto de dados. No entanto, todos os segmentos de dados referidos pelo snapshot precisarão ser bloqueados, mesmo se todos os arquivos capturados pelo snapshot forem excluídos após a captura do snapshot. A GC não pode recuperar o espaço que ainda é necessário para os snapshots; portanto, ter muitos snapshots pode fazer com que a taxa de compactação efetiva do sistema pareça baixa. Porém, os snapshots são recursos muito úteis de recuperação de falhas. Nós nunca devemos hesitar em capturar snapshots nem configurar agendamentos de snapshot adequados quando necessário.

3. Compactação: Estatísticas em linha

O DDOS realiza a desduplicação em linha, pois os dados são ingeridos pelo sistema. Ele monitora o efeito da desduplicação em linha e da compactação local em cada gravação e acumula as estatísticas no nível de arquivo. As estatísticas de compactação em linha por arquivo são agregadas ainda mais no nível da MTree e do sistema. A compactação é medida com base em três números das estatísticas em linha:

- O comprimento de cada gravação, chamado de *raw_bytes*;
- O comprimento de todos os segmentos exclusivos, chamado de *pre_lc_size*;
- O comprimento dos segmentos exclusivos compactados localmente, chamados de *post_lc_size*;

Com base nos três números acima, o DDOS define mais duas taxas de compactação de granularidade fina:

- *Compactação global (g_comp)*. É igual a (raw_bytes/pre_lc_size) e reflete a taxa de desduplicação;
- *Compactação local (l_comp)*. É igual a (pre_lc_size/post_lc_size) e reflete o efeito do algoritmo de compactação local.

As estatísticas acumuladas de compactação em linha fazem parte dos metadados de arquivo do DDOS e são armazenadas no inode de arquivo. O DDOS oferece recursos para verificar as compactações em linha em todos os três níveis: arquivo, MTree e o sistema inteiro. Nós os detalhamos nas seções abaixo.

3.1 Compactação de arquivos

A compactação de arquivos pode ser verificada pelo comando "filesys show compression <path>" da CLI, que informa as estatísticas acumuladas de compactação armazenadas no inode de arquivo. Quando um diretório é especificado, as estatísticas de compactação em linha de todos os arquivos contidos diretamente nesse diretório são resumidas e relatadas. No resultado da CLI, raw_bytes é identificado como "Original Bytes"; pre_lc_size é identificado como "Globally Compressed"; post_lc_bytes é identificado como "Locally Compressed"; e as outras sobrecargas são identificadas como "Meta-data". Os dois exemplos abaixo são capturados de um DDR real.
Exemplo 1: estatísticas de compactação em linha de um arquivo
filesys show compression /data/col1/main/dir1/file_1 Total files: 1; bytes/storage_used: 17.0 Original Bytes: 78,968,112 Globally Compressed: 7,805,052 Locally Compressed: 4,625,442 Meta-data: 24,820
Exemplo 2: estatísticas de compactação em linha de todos os arquivos de um diretório, inclusive todos os subdiretórios
filesys show compression /data/col1/main/dir1 Total files: 9; bytes/storage_used: 16.6 Original Bytes: 79,563,175 Globally Compressed: 8,081,177 Locally Compressed: 4,769,120 Meta-data: 27,408
O sistema informa a taxa geral de compactação em linha no resultado da CLI acima como "bytes/storage_used". No entanto, é necessário ter cuidado ao interpretar as informações acima, pois elas podem ser falsas por vários motivos. Um dos motivos é que pre_lc_size e post_lc_size são registrados quando as operações de dados são processadas. Quando os arquivos que, originalmente, adicionaram esses segmentos ao sistema são excluídos, o número de segmentos de dados exclusivos no arquivo restante deve aumentar.
Por exemplo, suponha que um arquivo sample.file seja submetido a backup em um sistema Data Domain e, no primeiro backup, as informações de compactação do arquivo são: pre_lc_size=10GiB, post_lc_size=5GiB. Em seguida, suponha que os dados desse arquivo são exclusivos, sem compartilhamento de dados com qualquer outro arquivo. No segundo backup do arquivo, suponha ainda que o arquivo receba uma desduplicação ideal, de modo que pre_lc_size e post_lc_size devem ser zero porque todos os segmentos do arquivo já existiam no sistema. Quando o primeiro backup é excluído, o segundo backup do arquivo se torna o único arquivo que faz referência aos 5 GiB de segmentos de dados. Nesse caso, o ideal é que pre_lc_size e post_lc_size do arquivo do 2º backup sejam atualizados de 0 para 10 GiB e 5 GiB, respectivamente.
No entanto, não há como detectar para quais arquivos isso deve ser feito; portanto, as estatísticas de compactação em linha dos arquivos existentes são deixadas inalteradas. Outro fato que afeta os números acima são as estatísticas acumuladas. Quando um arquivo recebe muitas substituições, não se sabe até que ponto as estatísticas acumuladas refletem as gravações que introduziram os dados em tempo real. Assim, com o passar de um longo período, as estatísticas de compactação em linha só podem ser tratadas como heurísticas para estimar aproximadamente a compactação de determinado arquivo.
Outro fato que vale a pena realçar é que a compactação em linha de um arquivo não pode ser medida para um intervalo de tempo arbitrário. Observe que as estatísticas de compactação em linha dos arquivos são um resultado acumulado e abrangem todas as gravações que o arquivo já recebeu. Quando um arquivo recebe muitas substituições, raw_bytes pode ser muito maior que o tamanho lógico do arquivo. Para arquivos fragmentados, os tamanhos de arquivo podem ser muito maiores que "Original Bytes".

3.2 Compactação de MTree

Nós podemos verificar a compactação de determinada MTree com o comando "*mtree show compression*" (MSC) da CLI. Há discussões segundo as quais os valores absolutos das estatísticas de compactação em linha são acumulados. Considerando-se que a vida útil de uma MTree pode ser muito longa, os valores absolutos se tornam cada vez menos informativos ao longo do tempo. Para resolver esse problema, nós usamos os deltas das estatísticas de compactação em linha e relatamos apenas as compactações de determinados intervalos de tempo. De acordo com a abordagem subjacente, nós fazemos o dump periódico das estatísticas de compactação em linha da MTree em um log. Quando um client consulta a compactação de MTree com o comando MSC da CLI, nós usamos o log para calcular os deltas dos números para a geração de relatórios de compactação. Por padrão, o MSC relata as compactações dos últimos 7 dias e das últimas 24 horas. Um usuário pode especificar qualquer período em que esteja interessado.
Vamos demonstrar os detalhes com um exemplo. Vamos supor que temos o seguinte log para a MTree A:
3:00AM, raw_bytes=11000GB, pre_lc_size=100GB, post_lc_size=50GB 4:00AM, raw_bytes=12000GB, pre_lc_size=200GB, post_lc_size=100GB
Então, a compactação da MTree A para essa hora é
g_comp = (12000-11000)/(200-100) = 10 l_comp = (200-100)/(100-50) = 2 overall compression ratio = (12000-11000)/(100-50) = 20
Claramente, o cálculo da taxa de compactação acima não realiza qualquer ação com o tamanho do conjunto de dados. Por exemplo, a MTree acima pode ter apenas dados lógicos de 500 GB.
O MSC oferece suporte à opção "daily" e "daily-detailed". O mesmo acontece com o comando "filesys show compression" da CLI. Quando a opção "daily" é especificada, a CLI relata a compactação diária com base em dias corridos. Ela usa os deltas diários de raw_bytes e post_lc_size para calcular a taxa de compactação diária. Quando a opção "daily-detailed" é especificada, a CLI mostra todos os três deltas (de raw_bytes, pre_lc_size e post_lc_size, respectivamente) de cada dia; ela também calcula os valores g_comp e l_comp, além de "Total Compression Factor".
Exemplos de resultados dos sistemas reais estão incluídos no Apêndice.

3.3 Compactação do sistema

Quando nós entendermos como a compactação é relatada nas MTrees, fica fácil estender o conceito para todo o sistema. A coleta e a geração de relatórios de estatísticas em linha da compactação de todo o sistema são exatamente iguais às das MTrees. A única diferença é o escopo, pois uma compactação é feita em uma MTree específica e, a outra, em todo o sistema. É possível verificar os resultados usando o comando "filesys show compression" da CLI. De fato, nós já incluímos um exemplo na Seção 2. A compactação do sistema com as opções "last 7 days" e "last 24 hours" é relatada nas duas últimas linhas da seção de resultados da saída do FSC.

4. GDA

GDA é a abreviação de "Global Deduplication Array" ou array global de desduplicação, em português. Trata-se de uma solução em cluster que pode incluir até dois nós. O GDA apresenta um espaço de armazenamento unificado aos usuários. As informações de compactação são agregadas de todos os nós. Portanto, nenhum elemento é tratado especialmente para fins de geração de relatórios de compactação. Teoricamente, nós podemos tratar um GDA como um sistema de único nó quando investigamos os relatórios de compactação de dados.

5. Arquivadores

Nos arquivadores, o armazenamento é separado em dois níveis: o nível ativo e o nível de arquivo. Eles são dois domínios independentes de desduplicação. O usuário só pode injetar dados no nível ativo. Posteriormente, um usuário pode usar os recursos de movimentação de dados oferecidos pelo DDOS para migrar dados do nível ativo para o nível de arquivo. Assim, a medição e a geração de relatórios de espaço e de compactação são processadas em cada nível. No entanto, com um arquivo por nível, nós não diferenciamos o nível e relatamos estatísticas de compactação em linha; elas são exatamente iguais às descritas na Seção 3.1.

6. Mistérios da desduplicação

O último tópico de destaque para entender a compactação do DDOS são as características da desduplicação, que é chamada de "compactação global" em muitos documentos do Data Domain. Embora a terminologia contenha a palavra "compactação", ela é totalmente diferente do conceito tradicional de compactação, que também é apresentado pelo DDOS com o nome "compactação local".

A compactação local simplesmente reduz o tamanho dos dados usando um algoritmo específico (observe que alguns tipos de dados não são compactáveis e a aplicação de algoritmos de compactação neles pode, na verdade, aumentar um pouco o tamanho dos dados). Geralmente, depois que um algoritmo é decidido, os dados em si são o único fator da taxa de compactação.

No entanto, a desduplicação é diferente. Ela não é um conceito local, e sim "*global*". Um segmento de dados recebido é desduplicado em todos os segmentos de dados existentes em um domínio de desduplicação, o que inclui todos os dados dos sistemas Data Domain não arquivadores. O segmento de dados em si não importa no procedimento de desduplicação.

Na prática, nós raramente vemos uma alta taxa de desduplicação no backup inicial de um conjunto de dados. Nos backups iniciais, muitas vezes, a grande redução de dados vem da compactação local. Quando os backups subsequentes chegam aos sistemas Data Domain, a desduplicação mostra sua força e se torna o fator dominante para a compactação. A eficácia da desduplicação depende do fato de que a taxa de alteração de um conjunto de dados geralmente é baixa de backup para backup. Por esse motivo, os conjuntos de dados com altas taxas de alteração podem não ser desduplicados satisfatoriamente. Quando o aplicativo de backup insere seus próprios fragmentos de metadados (chamados de marcadores pelo Data Domain) nas imagens de backup em uma frequência muito alta, ele também pode não obter uma boa taxa de desduplicação. Nossas técnicas de manuseio de marcadores podem ajudar em alguns casos, mas nem sempre.

Diante dessas observações, o que você deve esperar?

- Não se surpreenda quando os backups iniciais atingirem apenas uma pequena taxa de compactação efetiva do sistema, por exemplo, 2 ou 3. Geralmente, a desduplicação tem poucas oportunidades de mostrar sua força nos backups iniciais.
- A taxa de compactação global de um backup incremental é menor que a taxa de compactação do backup completo correspondente. Isso ocorre porque um backup incremental contém apenas arquivos alterados ou novos, em comparação com o backup anterior imediato. A taxa de compactação global depende da porcentagem de novos dados no backup incremental.
- A taxa de desduplicação de um backup completo (os não iniciais) também pode ser baixa em vários cenários. Alguns cenários observados com frequência são: uma grande porcentagem de dados é alterada, o conjunto de dados é dominado por arquivos pequenos, os aplicativos de backup adicionam muitos marcadores com espaçamento estreito, um backup de banco de dados é feito de modo incremental e/ou com tamanho pequeno de blocos etc. Quando uma baixa taxa de compactação é observada em um backup completo com baixa taxa de alteração de dados, nós precisamos verificar se esse é um dos casos que acabamos de descrever ou se é necessário envolver os desenvolvedores.
- Não suponha que a compactação da imagem de um backup posterior (arquivos) seja sempre melhor que a inicial. A imagem de um backup consecutivo pode mostrar uma alta taxa de desduplicação porque as imagens dos backups iniciais e anteriores já adicionaram a maioria dos dados ao sistema. Quando todas as imagens dos backups anteriores forem excluídas, a taxa de compactação global e local da imagem do backup mais antigo existente ainda poderá ser muito alta, mas ela só nos diz que a desduplicação foi satisfatória quando a imagem foi adicionada ao sistema, nada mais. Portanto, quando você exclui um arquivo, que tem uma taxa de compactação global e local muito alta e é a última imagem de backup de um conjunto de dados específico, você pode liberar muito mais espaço que o tamanho derivado da taxa de compactação.
- Não compare as taxas de compactação do mesmo conjunto de dados em sistemas diferentes, independentemente da forma como você adiciona o conjunto de dados: copiando por meio de protocolos como NFS e CIFS ou por replicação. Isso ocorre

porque cada sistema é um domínio de desduplicação independente. Não faz sentido comparar a taxa de desduplicação em diferentes domínios de desduplicação, até mesmo quando o conjunto de dados em questão é o mesmo.

7. Resumo

Medir a compactação é uma tarefa difícil em file systems de desduplicação, mas é ainda mais difícil em file systems de desduplicação estruturados por logs. Nós precisamos entender como a desduplicação funciona e como as estatísticas de compactação são monitoradas. As taxas de compactação são informações muito úteis para entender o comportamento de um sistema específico. A taxa de compactação efetiva do sistema é a medida mais importante, confiável e informativa. As estatísticas de compactação em linha também podem ser muito úteis, mas observe que podem não ser mais do que heurísticas em algumas circunstâncias. Claramente, ainda há áreas para aprimorar o monitoramento e a geração de relatórios de compactação. No entanto, o DDOS já faz um trabalho razoavelmente bom em geral.

Apêndice. Exemplos de resultados de Mtree Show Compression

Vamos supor que exista uma MTree que contém 254.792,4 GiB de dados do usuário. Ela recebeu apenas 4.379,3 GiB de novos dados nos últimos 7 dias e 78,4 GiB de novos dados nas últimas 24 horas, respectivamente. Obviamente, é possível especificar outros intervalos de tempo. A opção "*daily*" informa as estatísticas de compactação em linha dos últimos 33 dias. Quando a opção "*daily-detailed*" é definida, as taxas totais de compactação são mais detalhadas, separando-as em taxas de compactação global e local.
 # mtree list /data/col1/main Name Pre-Comp (GiB) Status ———— ———— —— /data/col1/main 254792.4 RW ———— ———— —— D : Deleted RO : Read Only RW : Read Write RD : Replication Destination RLE : Retention-Lock Enabled RLD : Retention-Lock Disabled
 # mtree show compression /data/col1/main From: 2012-06-07 14:00 To: 2012-06-14 14:00 No data available for the selected interval. Pre-Comp Post-Comp Global-Comp Local-Comp Total-Comp (GiB) (GiB) Factor Factor Factor (Reduction %) ———— —— —— —— —— ———— ———— Written:* Last 7 days 4379.3 883.2 3.4x 1.5x 5.0x (79.8) Last 24 hrs 784.6 162.1 3.3x 1.4x 4.8x (79.3) ———— —— —— —— —— ———— ———— * Does not include the effects of pre-comp file deletes/truncates since the last cleaning on 2011/03/19 16:09:04. Key: Pre-Comp = Data written before compression Post-Comp = Storage used after compression Global-Comp Factor = Pre-Comp / (Size after de-dupe) Local-Comp Factor = (Size after de-dupe) / Post-Comp Total-Comp Factor = Pre-Comp / Post-Comp Reduction % = ((Pre-Comp - Post-Comp) / Pre-Comp) * 100
 # mtree show compression /data/col1/main daily From: 12/05/2012 12:00 To: 2012-06-14 12:00 Sun Mon Tue Wed Thu Fri Sat Weekly - —— —— —— —— —— —— —— ———— -13- -14- -15- -16- -17- -18- -19- Date 432.0 405.9 284.1 438.8 347.0 272.7 331.4 2511.8 Pre-Comp 85.5 66.2 45.3 81.9 61.4 57.4 66.3 464.1 Post-Comp 5.0x 6.1x 6.3x 5.4x 5.7x 4.7x 5.0x 5.4x Total-Comp Factor -20- -21- -22- -23- -24- -25- -26- 478.0 387.8 450.2 533.1 386.0 258.4 393.6 2887.1 100.6 81.5 100.8 119.0 84.0 40.6 75.3 601.8 4.8x 4.8x 4.5x 4.5x 4.6x 6.4x 5.2x 4.8x -27- -28- -29- -30- -31- -1- -2- 27.6 1.0 0.4 470.7 467.3 517.7 641.9 2126.7 4.9 0.2 0.1 83.9 92.3 89.8 140.1 411.2 5.6x 5.6x 4.3x 5.6x 5.1x 5.8x 4.6x 5.2x -3- -4- -5- -6- -7- -8- -9- 539.6 495.0 652.8 658.7 537.1 398.7 305.5 3587.3 110.8 108.0 139.4 137.0 111.5 78.3 48.3 733.3 4.9x 4.6x 4.7x 4.8x 4.8x 5.1x 6.3x 4.9x -10- -11- -12- -13- -14- 660.2 738.3 787.2 672.9 796.9 3655.5 143.9 152.5 167.6 126.9 163.3 754.2 4.6x 4.8x 4.7x 5.3x 4.9x 4.8x —— —— —— —— —— —— —— —— ———— Pre-Comp Post-Comp Global-Comp Local-Comp Total-Comp (GiB) (GiB) Factor Factor Factor (Reduction %) ———— —— —— —— —— —— ———— Written:* Last 33 days 14768.3 2964.5 3.4x 1.5x 5.0x (79.9) Last 24 hrs 784.6 162.1 3.3x 1.4x 4.8x (79.3) ———— —— —— —— —— —— ———— * Does not include the effects of pre-comp file deletes/truncates since the last cleaning on 2011/03/19 16:09:04. Key: Pre-Comp = Data written before compression Post-Comp = Storage used after compression Global-Comp Factor = Pre-Comp / (Size after de-dupe) Local-Comp Factor = (Size after de-dupe) / Post-Comp Total-Comp Factor = Pre-Comp / Post-Comp Reduction % = ((Pre-Comp - Post-Comp) / Pre-Comp) * 100
 # mtree show compression /data/col1/main daily-detailed From: 12/05/2012 12:00 To: 2012-06-14 12:00 Sun Mon Tue Wed Thu Fri Sat Weekly —— —— —— —— —— —— —— —— ———— -13- -14- -15- -16- -17- -18- -19- Date 432.0 405.9 284.1 438.8 347.0 272.7 331.4 2511.8 Pre-Comp 85.5 66.2 45.3 81.9 61.4 57.4 66.3 464.1 Post-Comp 3.5x 4.1x 4.3x 3.6x 3.8x 3.3x 3.4x 3.7x Global-Comp Factor 1.4x 1.5x 1.5x 1.5x 1.5x 1.4x 1.5x 1.5x Local-Comp Factor 5.0x 6.1x 6.3x 5.4x 5.7x 4.7x 5.0x 5.4x Total-Comp Factor 80.2 83.7 84.1 81.3 82.3 78.9 80.0 81.5 Reduction % -20- -21- -22- -23- -24- -25- -26- 478.0 387.8 450.2 533.1 386.0 258.4 393.6 2887.1 100.6 81.5 100.8 119.0 84.0 40.6 75.3 601.8 3.3x 3.3x 3.0x 3.0x 3.3x 4.1x 3.6x 3.3x 1.4x 1.5x 1.5x 1.5x 1.4x 1.5x 1.4x 1.5x 4.8x 4.8x 4.5x 4.5x 4.6x 6.4x 5.2x 4.8x 79.0 79.0 77.6 77.7 78.2 84.3 80.9 79.2 -27- -28- -29- -30- -31- -1- -2- 27.6 1.0 0.4 470.7 467.3 517.7 641.9 2126.7 4.9 0.2 0.1 83.9 92.3 89.8 140.1 411.2 4.4x 3.7x 2.6x 3.8x 3.5x 3.9x 3.2x 3.5x 1.3x 1.5x 1.6x 1.5x 1.4x 1.5x 1.5x 1.5x 5.6x 5.6x 4.3x 5.6x 5.1x 5.8x 4.6x 5.2x 82.1 82.2 76.8 82.2 80.3 82.7 78.2 80.7 -3- -4- -5- -6- -7- -8- -9- 539.6 495.0 652.8 658.7 537.1 398.7 305.5 3587.3 110.8 108.0 139.4 137.0 111.5 78.3 48.3 733.3 3.4x 3.1x 3.2x 3.4x 3.3x 3.4x 4.1x 3.3x 1.4x 1.5x 1.5x 1.4x 1.4x 1.5x 1.6x 1.5x 4.9x 4.6x 4.7x 4.8x 4.8x 5.1x 6.3x 4.9x 79.5 78.2 78.6 79.2 79.2 80.4 84.2 79.6 -10- -11- -12- -13- -14- 660.2 738.3 787.2 672.9 796.9 3655.5 143.9 152.5 167.6 126.9 163.3 754.2 3.1x 3.4x 3.2x 3.7x 3.4x 3.3x 1.5x 1.4x 1.5x 1.4x 1.5x 1.5x 4.6x 4.8x 4.7x 5.3x 4.9x 4.8x 78.2 79.3 78.7 81.1 79.5 79.4 —— —— —— —— —— —— —— —— ———— Pre-Comp Post-Comp Global-Comp Local-Comp Total-Comp (GiB) (GiB) Factor Factor Factor (Reduction %) ———— —— —— —— —— —— ———— Written:* Last 33 days 14768.3 2964.5 3.4x 1.5x 5.0x (79.9) Last 24 hrs 784.6 162.1 3.3x 1.4x 4.8x (79.3) ———— —— —— —— —— —— ———— * Does not include the effects of pre-comp file deletes/truncates since the last cleaning on 2011/03/19 16:09:04. Key: Pre-Comp = Data written before compression Post-Comp = Storage used after compression Global-Comp Factor = Pre-Comp / (Size after de-dupe) Local-Comp Factor = (Size after de-dupe) / Post-Comp Total-Comp Factor = Pre-Comp / Post-Comp Reduction % = ((Pre-Comp - Post-Comp) / Pre-Comp) * 100

Propriedades do artigo

Produto afetado

Data Domain

Produto

Data Domain

Data da última publicação

21 abr 2021

Versão

3

Tipo de artigo

How To

Dell EMC DD and PowerProtect Hardware 7.7

Features and Specifications

7.7

December 2021
Rev. 01

DELL Technologies

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

Figures

Tables

1

Physical and Environmental Requirements

This chapter contains the following topics:

Topics:

- System operating limits
- Air quality requirements
- Shipping and storage requirements
- Shock and vibration

System operating limits

The ambient temperature specification is measured at the front bezel inlet. The site must have air conditioning of the correct size and placement to maintain the specified ambient temperature range and offset the heat dissipation listed below.

NOTE: For systems mounted in a cabinet, the operating limits listed above must not be exceeded inside the closed cabinet. Equipment mounted directly above or below an enclosure must not restrict the front-to-rear airflow of the storage system. Cabinet doors must not impede the front-to-rear airflow. The cabinet must exhaust air at a rate that is equal to or greater than the sum of the exhaust rates of all the equipment mounted in the cabinet.

Environmental recovery

If the system exceeds the maximum ambient temperature by approximately 10°C (18°F), the storage processors (SPs) in the processor enclosure begin an orderly shutdown that saves cached data, and then shut themselves down. Link control cards (LCCs) in each DAE power down their disks but remain powered on. If the system detects that the temperature has dropped to an acceptable level, it restores power to the SPs and the LCCs restore power to their disk drives.

Air quality requirements

The products are designed to be consistent with the requirements of the American Society of Heating, Refrigeration and Air Conditioning Engineers (ASHRAE) Environmental Standard Handbook and the most current revision of Thermal Guidelines for Data Processing Environments, Second Edition, ASHRAE 2009b.

Cabinets are best suited for Class 1 datacom environments, which consist of tightly controlled environmental parameters, including temperature, dew point, relative humidity and air quality. These facilities house mission-critical equipment and are typically fault-tolerant, including the air conditioners.

The data center should maintain a cleanliness level as identified in ISO 14664-1, class 8 for particulate dust and pollution control. The air entering the data center should be filtered with a MERV 11 filter or better. The air within the data center should be continuously filtered with a MERV 8 or better filtration system. In addition, efforts should be maintained to prevent conductive particles, such as zinc whiskers, from entering the facility.

The allowable relative humidity level is 20 to 80% non condensing, however, the recommended operating environment range is 40 to 55%. For data centers with gaseous contamination, such as high sulfur content, lower temperatures and humidity are recommended to minimize the risk of hardware corrosion and degradation. In general, the humidity fluctuations within the data center should be minimized. It is also recommended that the data center be positively pressured and have air curtains on entry ways to prevent outside air contaminants and humidity from entering the facility.

For facilities below 40% relative humidity, it is recommended to use grounding straps when contacting the equipment to avoid the risk of Electrostatic discharge (ESD), which can harm electronic equipment.

As part of an ongoing monitoring process for the corrosiveness of the environment, it is recommended to place copper and silver coupons (per ISA 71.04-1985, Section 6.1 Reactivity), in airstreams representative of those in the data center. The monthly reactivity rate of the coupons should be less than 300 Angstroms. When monitored reactivity rate is exceeded, the coupon should be analyzed for material species and a corrective mitigation process put in place.

Storage time (unpowered) recommendation: do not exceed 6 consecutive months of unpowered storage.

Shipping and storage requirements

NOTE: Systems and components must not experience changes in temperature and humidity that are likely to cause condensation to form on or in that system or component. Do not exceed the shipping and storage temperature gradient of 45°F/hr (25°C/hr).

Table 1. Shipping and storage requirements

Requirement	Description
Ambient temperature	-40° F to 149°F (-40°C to 65°C)
Temperature gradient	45°F/hr (25°C/hr)

Table 1. Shipping and storage requirements (continued)

Requirement	Description
Relative humidity	10% to 90% noncondensing
Elevation	-50 to 35,000 ft (-16 to 10,600 m)
Storage time (unpowered) Recommendation	Do not exceed 6 consecutive months of unpowered storage.

Shock and vibration

Products have been tested to withstand the shock and random vibration levels. The levels apply to all three axes and should be measured with an accelerometer on the equipment enclosures within the cabinet and shall not exceed:

Platform condition	Response measurement level
Non operational shock	10 G's, 7 ms duration
Operational shock	3 G's, 11 ms duration
Non operational random vibration	0.40 Grms, 5-500 Hz, 30 minutes
Operational random vibration	0.21 Grms, 5-500 Hz, 10 minutes

Systems that are mounted on an approved package have completed transportation testing to withstand the following shock and vibrations in the vertical direction only and shall not exceed:

Packaged system condition	Response measurement level
Transportation shock	10 G's, 12ms duration
Transportation random vibration	• 1.15 Grms • 1 hour Frequency range 1-200 Hz

2

DD3300

This chapter contains the following topics:

Topics:

- DD3300 system features
- DD3300 system specifications
- DD3300 storage capacity
- Front panel
- Rear panel

DD3300 system features

Table 2. DD3300 system features

Feature	4 TB configuration	8 TB configuration	16 TB configuration	32 TB configuration
Rack Height	2U, supported in four-post racks only			
Power	1 or 2 hot-swappable power units			
Fans	6 hot swappable fans, installed in two fan assemblies (3 fans per fan assembly)			
Rack mounting	Rack mount kit included with each system. Adjustable between 24 - 36 in. (60.9–76.2 cm).			
Processor	1 x 8-core Intel 4110 series, hyperthreaded			
Voltage	100–240 V~. Frequency: 50 Hz to 60 Hz.			
Internal 3.5" drives (front)	4 x 4 TB HDD	10 x 4 TB HDD	10 x 4 TB HDD	12 x 4 TB HDD
Internal 3.5" drives (middle)	N/A	N/A	N/A	4 x 4 TB HDD
Internal 3.5" drives (rear)	N/A	1 x 480 GB SSD for NVRAM[a]		
NIC	4 x 1 GbE or 4 x 10 GbE (always present)[b] + 2 x 10 GbE (optional)			
FC (DD VTL only)	4 x 16 Gbps (optional)			
Memory	16 GB or 24 GB[c]	48 GB	48 GB or 56 GB[d]	64 GB

a. The SSD is for use as an NVRAM device, SSD Cache Tier storage only, and Random I/O handling (Instant Access Instant Restore). The maximum supported SSD Cache Tier capacity is one percent of the Active Tier capacity.
b. Starting with DD OS 6.2, DD3300 systems ship with a 4 x 10 GbE RJ-45 network daughter card.
c. 24 GB of memory is required to use the FC module for DD VTL.
d. A 16 TB system will have 56 GB of memory if it was a 4 TB system equipped with the FC module, and was later upgraded to 16 TB.

NOTE: DD OS may report less storage and memory than indicated in this table. The unreported resources are used for internal system processes.

DD3300 system specifications

Table 3. DD3300 system specifications

Watts	BTU/hr	Weight	Width	Depth	Height
750	2891	72.91 lb/33.1 kg	17.09 in/43.4 cm	28.17 inches/71.55 cm	3.42 in/8.68 cm

Table 4. System operating environment

Operating Temperature	50° to 95° F (10° to 35° C), derate 1.1° C per 1000 feet, above 7500 feet up to 10,000 feet
Operating Humidity	20% to 80%, non-condensing
Non-operating Temperature	-40° to +149° F (-40° to +65° C)

Table 4. System operating environment (continued)

Operating Acoustic Noise	Sound power, LWAd: 7.52 bels. Sound pressure, LpAm: 56.4 dB. (Declared noise emission per ISO 9296.)

DD3300 storage capacity

The table lists the capacities of the systems. The system internal indexes and other product components use variable amounts of storage, depending on the type of data and the sizes of files. If you send different datasets to otherwise identical systems, one system may, over time, have room for more or less actual backup data than another.

Table 5. DD3300 storage capacity

Configuration	Internal disks - physical[a][b]	Internal disks - virtual	Raw storage	Usable storage (local)[c]	Cloud storage	SSD metadata cache storage
4 TB capacity /16 GB memory	4 x 4 TB 7200 RPM NLSAS	• 1 x 4 TB for Active Tier • 1 x 1 TB for DD Cloud Tier metadata	16 TB	4 TB	8 TB	N/A
8 TB capacity/48 GB memory	10 x 4 TB 7200 RPM NLSAS	• 4 x 4 TB for Active Tier[d] • 2 x 1 TB for DD Cloud Tier metadata	40 TB	8 TB	16 TB	160 GB
16 TB capacity/48 GB memory	10 x 4 TB 7200 RPM NLSAS	• 4 x 4 TB for Active Tier • 2 x 1 TB for DD Cloud Tier metadata	40 TB	16 TB	32 TB	160 GB
32 TB capacity/64 GB memory	• 12 x 4 TB 7200 RPM NLSAS (front) • 4 x 4 TB 7200 RPM NLSAS (middle)	• 8 x 4 TB for Active Tier • 4 x 1 TB for DD Cloud Tier metadata	64 TB	32 TB	64 TB	320 GB

a. The internal hard drives are configured in a RAID6 configuration. RAID6 provides the system with the ability to withstand the simultaneous failure of two hard drives, or the failure of one hard drive while another hard drive is still rebuilding after a drive replacement operation.
b. After replacing a disk, it takes approximately 18 hours to complete the rebuild operation on the new disk, but may take longer depending on the amount of activity on the system.
c. The system compensates for the required file system overhead, so the reported usable capacity matches the specified usable capacity.
d. For 8 TB configurations, the Active Tier supports a maximum of 2 x 4 TB virtual disks.

Front panel

The DD3300 front panel consists of two control panels, which contain system LEDs and ports, twelve 3.5" disk drive bays, and the service tag. Front panel shows the locations of the front panel components.

Figure 1. Front panel

1. Left control panel
2. 3.5" disk drive
3. Right control panel
4. Service tag.

Disk layout

The following table shows the physical location of each disk slot.

NOTE: Although the physical slots are numbered starting from 0, the software identifies the slots starting at 1.

Table 6. Front disk slot numbers

Slot 0 (SW slot 1)	Slot 3 (SW slot 4)	Slot 6 (SW slot 7)	Slot 9 (SW slot 10)
Slot 1 (SW slot 2)	Slot 4 (SW slot 5)	Slot 7 (SW slot 8)	Slot 10 (SW slot 11)
Slot 2 (SW slot 3)	Slot 5 (SW slot 6)	Slot 8 (SW slot 9)	Slot 11 (SW slot 12)

Left control panel

The left control panel contains system status LEDs. Left control panel shows the panel.

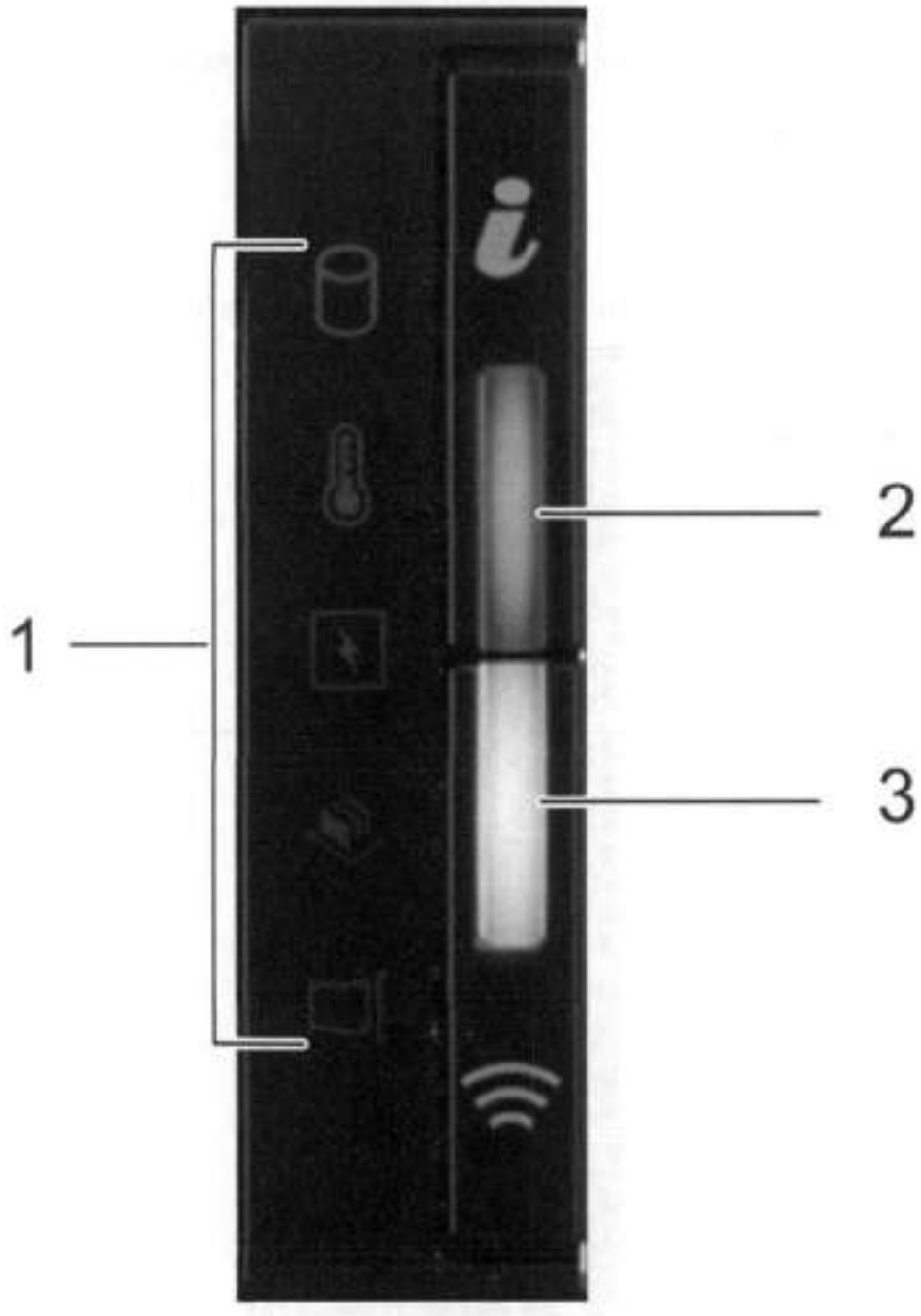


Figure 2. Left control panel

1. System status LEDs
2. System health and system ID indicator
3. iDRAC Quick Sync 2 wireless indicator (Not supported)

The system status LEDs turn solid amber if the system experiences an error in any of the following categories. Under normal operating conditions, the system status LEDs remain off. From top to bottom, the five system status LEDs are:

- Drive indicator
- Temperature indicator
- Electrical indicator
- Memory indicator
- PCIe indicator

The system health and system ID indicator has the following states:

- Solid blue: Indicator is in system health mode. System is on and healthy.
- Blinking blue: Indicator is in system ID mode.

  NOTE: Press the System Health and System ID button to switch the indicator between system health and system ID modes.
- Solid amber: System is in fail-safe mode.
- Blinking amber: System is experiencing a fault.

Right control panel

The right control panel contains the system power button, and system maintenance ports. Right control panel shows the panel.

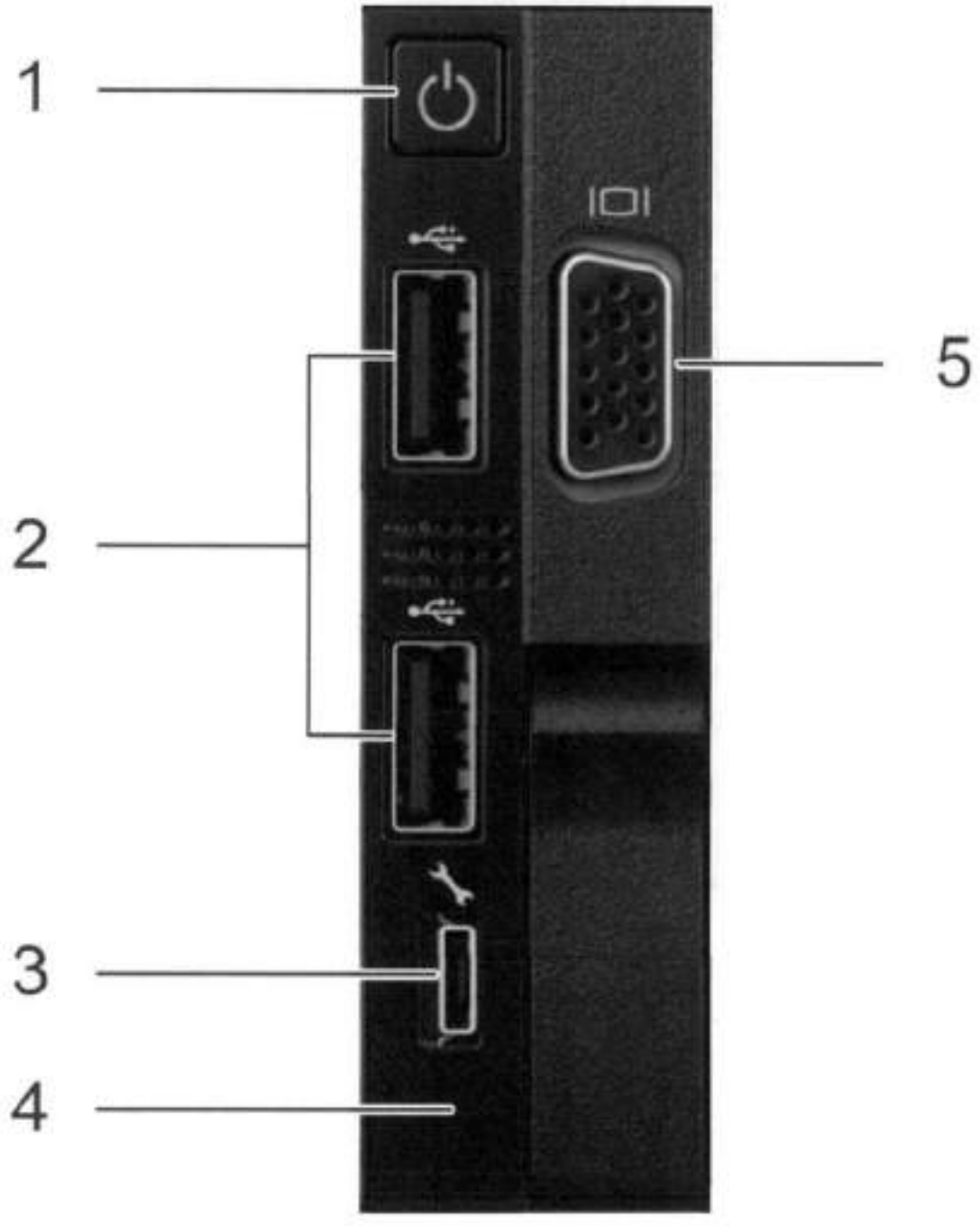


Figure 3. Right control panel

1. Power button

2. Not Supported -- 2 x USB 2.0 ports (Not supported)
3. Not Supported -- iDRAC Direct port (micro USB 2.0)
4. iDRAC Direct LED
5. Not Used -- VGA port

Front disks

The DD3300 system contains 4, 10, or 12 front-mounted 3.5" HDDs, depending on the capacity configuration. Each HDD has an activity indicator, and a status indicator. Disk LEDs shows the HDD indicators.

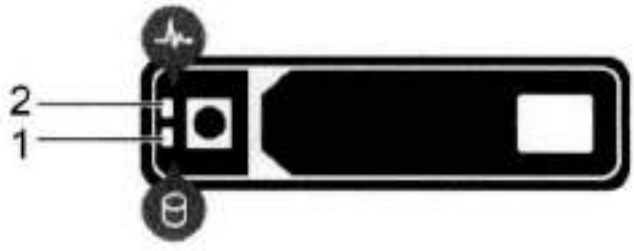


Figure 4. Disk LEDs

1. HDD activity indicator
2. HDD status indicator

The HDD activity indicator blinks during drive activity.

The HDD status indicator has the following states:

- Flashes green twice per second: Identifying drive or preparing for removal.
- Off: Drive is ready for removal.
- Flashes green, then amber, then turns off: Predicted drive failure.
- Flashes amber four times per second: Drive failed.
- Solid green: Drive online.
- Flashes green slowly: Drive rebuilding.
- Flashes green for three seconds, then amber for three seconds, then turns off: Rebuild stopped.

Service tag

The DD3300 system service tag is located at the front of the system, in the lower right-hand corner of the chassis. This tag is on all DD3300 systems, and includes the product serial number.

Figure 5. Service tag

1. Information tag (top view)
2. Information tag (back view)
3. OpenManage Mobile (OMM) label
4. iDRAC MAC address and secure password label
5. Service tag

Rear panel

The DD3300 rear panel contains the system serial port, NIC cards, power supplies, and 3.5" drive bays. shows the rear of the system.

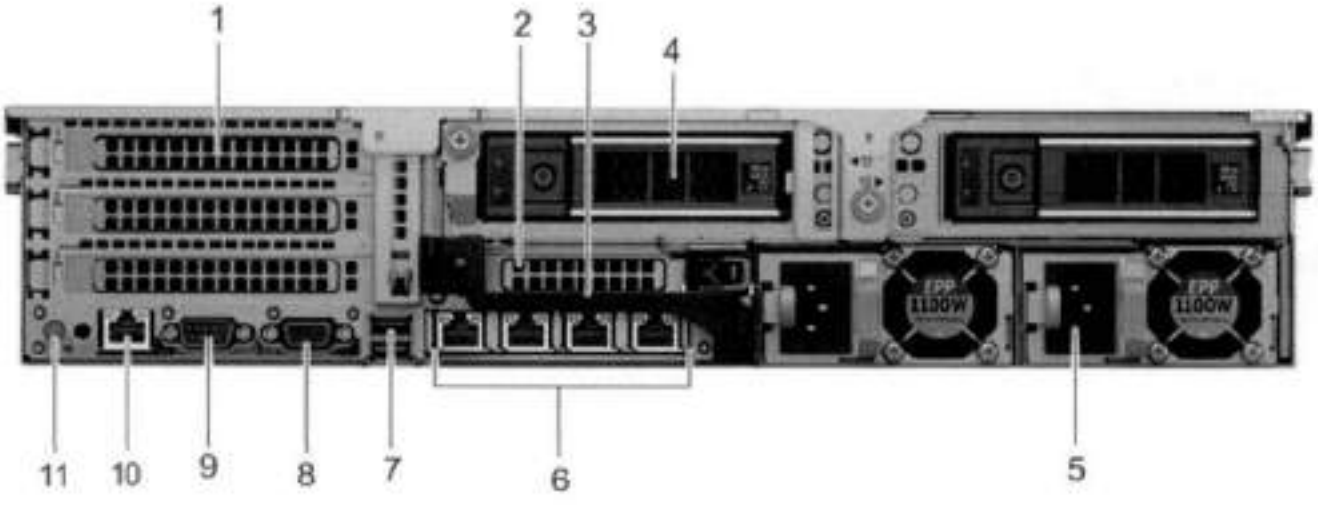


Figure 6. Rear panel

1. Full height PCIe expansion card slots
   - The top slot is for the optional 2 x 10 GbE NIC
   - The middle slot is for the optional 4 x 16 Gbps FC module
   - The bottom slot is not supported
2. Not Supported -- Half height PCIe expansion card slot
3. Rear handle
4. 3.5" drive bays (used for 1 x 480 GB SSD in the 8 TB, 16 TB, and 32 TB configurations)
5. Power supply units (1 or 2)

3. Network daughter card Ethernet ports
7. Not Supported — USB 3.0 ports
8. Not Supported — VGA port
9. Serial port
10. iDRAC9 dedicated management port
11. System identification button

The DD3300 system supports the use of the iDRAC9 dedicated management port to emulate a serial console.

Disk layout

8 TB, 16 TB, and 32 TB configurations use one rear slot for an SSD. 4 TB configurations do not use an SSD. The following table shows the physical location of the rear SSD slots.

NOTE: Although the physical slots are numbered starting from 0, the software identifies the slots starting at 1.

Table 7. Rear disk slot numbers

Slot 12 (SW slot 13)	Slot 13 (SW slot 14)

Network port layout

The DD3300 network daughter card provides 4 x 1 GbE or 4 x 10 GbE network ports for network connectivity.

NOTE: Starting with DD OS 6.2, DD3300 systems ship with a 4 x 10 GbE RJ-45 network daughter card.

The following table lists the layout of the network daughter card ports.

Table 8. Network daughter card port identifiers

ethMa	ethMb	ethMc	ethMd

An optional 2 x 10 GbE module is supported on the DD3300 system.

Figure 7. 2 x 10 GbE module

The following table lists the layout of the 10 GbE ports.

NOTE: The 10 GbE module is inserted upside down, therefore the ports are in descending order from left to right.

Table 9. Optional 10 GbE module port identifiers

eth1b	eth1a

FC port layout

An optional 4 x 16 Gbps FC module is supported on the DD3300 system.

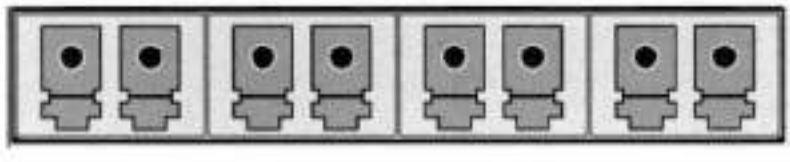


Figure 8. 4 x 16 Gbps FC module

The following table lists the layout of the FC ports.

Table 10. Optional 16 Gbps FC module port identifiers

22d	22c	22b	22a

Product serial number tag (PSNT)

Some DD3300 systems have a PSNT tag located on the rear of the system, attached to the arm in the center of the chassis. If this tag is not present, the product serial number is always available from the service tag located on the front of the system.

NOTE: Service tag describes the front-mounted service tag.

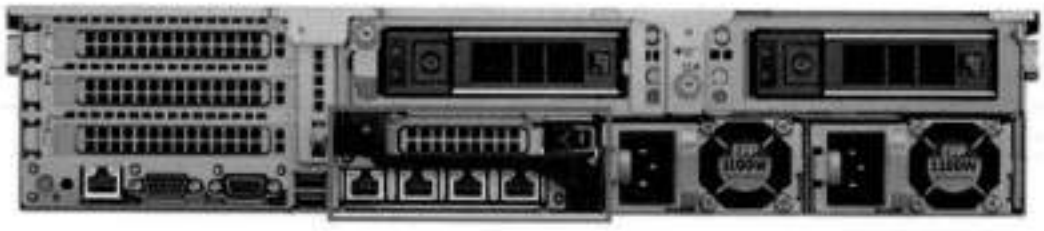


Figure 9. PSNT location

If present, the PSNT lists the part number (PN) and serial number (SN) of the system. The PN is 900-565-024. The SN is the 14 digit alphanumeric string that accompanies the part number. This serial number is the default system password for serial console, system manager, and iDRAC access.

Rear SSD

The DD3300 8 TB, 16 TB, and 32 TB configurations use one rear-mounted 480 GB 2.5" SSD. The SSD has an activity indicator, and a status indicator.

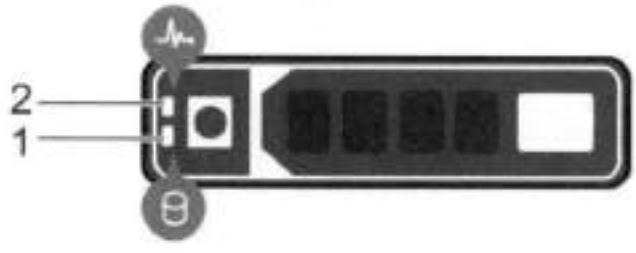


Figure 10. Disk LEDs

1. HDD activity indicator
2. HDD status indicator

The HDD activity indicator blinks during drive activity.

The HDD status indicator has the following states:

- Flashes green twice per second: Identifying drive or preparing for removal.
- Off: Drive is ready for removal.
- Flashes green, then amber, then turns off: Predicted drive failure.
- Flashes amber four times per second: Drive failed.
- Solid green: Drive online.

NIC indicators

All network ports on the DD3300 system have link and activity LED indicators.

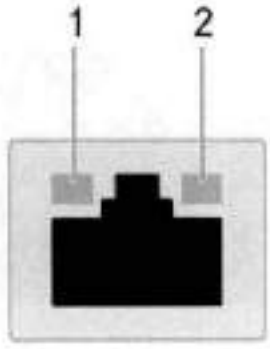


Figure 11. NIC LEDs

1. Link LED indicator
2. Activity LED indicator

The NIC LEDs have the following states:

Table 11. NIC LED states

Link indicator state	Activity indicator state	Meaning
Green	Blinking green	The NIC is connected to a valid network at its maximum port speed and data is being sent or received.
Amber	Blinking green	The NIC is connected to a valid network at less than its maximum port speed and data is being sent or received.
Green	Off	The NIC is connected to a valid network at its maximum port speed and data is not being sent or received.
Amber	Off	The NIC is connected to a valid network at less than its maximum port speed and data is not being sent or received.
Blinking green	Off	NIC identify is enabled through the NIC configuration utility.

Power supply indicators

The power supply unit has an illuminated, translucent handle that functions as a status LED.

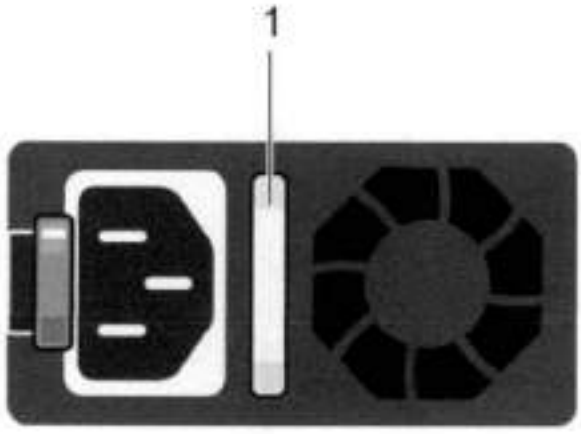


Figure 12. Power supply LED

The indicator has the following states:

- Green: Valid power source is connected, and the PSU is operational.
- Blinking amber: Indicates a problem with the PSU.
- Off: Power is not connected.
- Blinking green: Firmware update is in progress.

  CAUTION: **Do not disconnect the power cord or unplug the PSU when updating firmware. If firmware update is interrupted, the PSUs do not function.**
- Blinking green, then off: When hot-plugging a PSU, the PSU handle blinks green five times at a rate of 4 Hz and turns off. This indicates a PSU mismatch with respect to efficiency, feature set, health status, or supported voltage.

3

DD4200

This chapter contains the following topics:

Topics:

- DD4200 system features
- DD4200 system specifications
- DD4200 storage capacity
- Front Panel
- Back Panel
- I/O modules and slot assignments
- Internal system components
- DD4200 and ES30 shelf guidelines
- DD4200 and DS60 shelf guidelines

DD4200 system features

The table summarizes the DD4200 system features.

Table 12. DD4200 system features

Feature		DD4200 (Base configuration)
Rack height		4U, supported in four-post racks only
Rack mounting		Rack mount kit included with each system. Adjustable between 24 - 36 in. (60.9 - 76.2 cm).
Power		1 +1 redundant, hot-swappable power units
Processor		Two 8-core processors
NVRAM		One 4-GB NVRAM module (and companion BBU) for data integrity during a power outage
Fans		Hot-swappable, redundant, 5
Memory		16 x 8 GB DIMM (128 GB)
Internal drives		SSD drives, 3 x 200 GB (base 10)
I/O module slots		Nine replaceable I/O module (Fibre Channel, Ethernet, and SAS) slots, one BBU, one NVRAM, and one Management module slot. See Management module and interfaces and I/O modules and slot assignments.
Supported capacity	Non-extended retention	8 x 2-TB or 5 x 3-TB shelves adding up to 189 TB of usable external capacity.
	DD Cloud Tier	189 TB of Active Tier capacity, and 378 TB of Cloud Tier capacity. 2x3 TB shelves are required to store DD Cloud Tier metadata.
	DD Extended Retention	24 x 2-TB or 16 x 3-TB shelves adding up to 378 TB of usable external capacity. If lower-capacity 1 TB-drive-based shelves are used, the maximum configuration will also be limited by a maximum shelf count of 32.

DD4200 system specifications

Table 13. DD4200 system specifications

Model	Watts	BTU/hr	Power	Weight	Width	Depth	Height
DD4200	800	2730	800	80 lb / 36.3 kg	17.5 in (44.5 cm)	33 in (84 cm)	7 in (17.8 cm)

Table 14. System operating environment

Operating Temperature	50° to 95° F (10° to 35° C), derate 1.1° C per 1000 feet, above 7500 feet up to 10,000 feet
Operating Humidity	20% to 80%, non-condensing
Non-operating Temperature	-40° to +149° F (-40° to +65° C)
Operating Acoustic Noise	Sound power, LWAd: 7.52 bels. Sound pressure, LpAm: 56.4 dB. (Declared noise emission per ISO 9296.)

DD4200 storage capacity

Data Domain system internal indexes and other product components use variable amounts of storage, depending on the type of data and the sizes of files. If you send different data sets to otherwise identical systems, one system may, over time, have room for more or less actual backup data than another.

Table 15. DD4200 storage capacity

System/ Installed Memory	Internal Disks (SATA SSDs)	Data Storage Space	External Storage[3]
DD4200 (2 SAS I/O modules) 128 GB	2.5 in. 3 @ 200 GB No User Data	189 TB	Up to a maximum of 8 x 2-TB or 5 x 3-TB shelves.
DD4200 with DD Cloud Tier[1] (3 SAS I/O modules) 128 GB	2.5 in. 3 @ 200 GB No User Data	• 189 TB (Active Tier) • 72 TB (DD Cloud Tier metadata) • 378 TB (DD Cloud Tier)	Up to a maximum of 8 x 2-TB or 5 x 3-TB shelves. 2x3-TB shelves for DD Cloud Tier metadata.
DD4200 with Extended Retention software[1] (4 SAS I/O modules) 128 GB	2.5 in. 3 @ 200 GB No User Data	378 TB	Up to a maximum of 16 x 2-TB and 10 x 3-TB shelves.

1. Data Domain DD4200 controller with DD Extended Retention software.

2. Data Domain DD4200 controller with DD Cloud Tier.

3. The capacity will differ depending on the size of the external storage shelves used. This data based on ES30 shelves.

Front Panel

The photo shows the hardware features and interfaces on the front of the system.

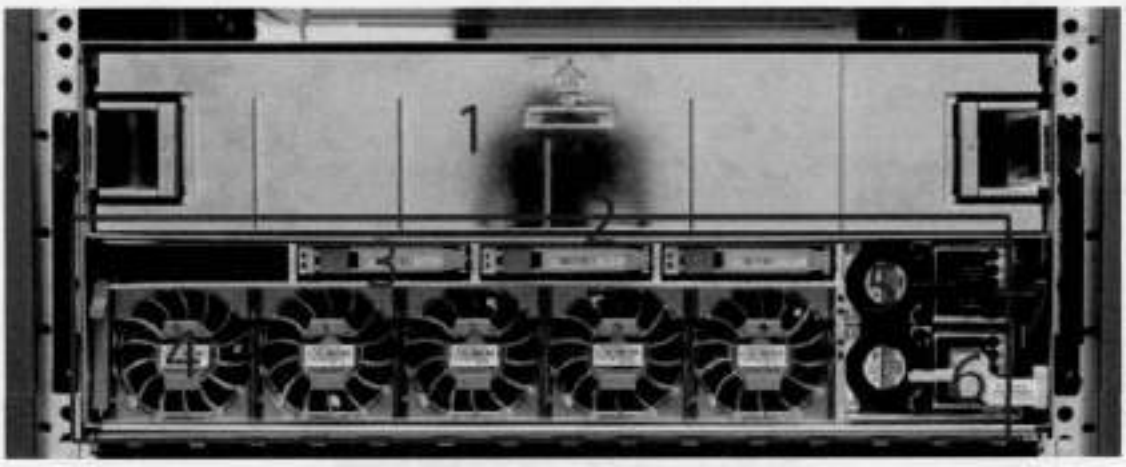


Figure 13. Front panel components

(1)	Filler panel
(2)	The red box indicates the system processor (SP) module
(3)	SSD drive #1
(4)	Fan #0
(5)	Power supply #B
(6)	AC power disconnect plug
(7)	AC power extender module

Power supply units

A system has two power supply units, numbered A and B from the bottom up. Each power supply has its own integral cooling fan. Each power unit has three LEDs (see System LED legend label) that indicates the following states:

- AC LED: Glows green when AC input is good
- DC LED: Glows green when DC output is good
- Symbol "!": Glows solid or blinking amber for fault or attention

The AC power plugs are located to the right of each power supply. These plugs are pulled to disconnect AC power to each power supply.

AC power extender module

AC power entry is connected at the rear of the system. The AC power extender module provides power to the two power supplies on the front of the system. AC Power plugs are located in the front. The module is adjacent to the SP module and can be removed and replaced.

Cooling Fans

A system contains five hot-swappable cooling fans in a 4+1 redundant configuration. The fans provide cooling for the processors, DIMMs, IO modules, and the management module. Each fan has a fault LED which causes the fan housing to glow amber. A system can run with one fan faulted or removed.

Solid-state drives

A system contains three hot-swappable 2.5" solid-state drive (SSD) bays that are located in the front and on top of the fan modules. There are four drive bays, with the left-most bay containing a blank. The next drive to the right of the blank is SSD #1, the next is #2, and the right-most bay contains SSD #3. No user backup data is kept on the SSDs.

Each drive has a blue colored power LED and an amber fault LED.

Front LED Indicators

The photo below indicates the location of the four system LEDs.

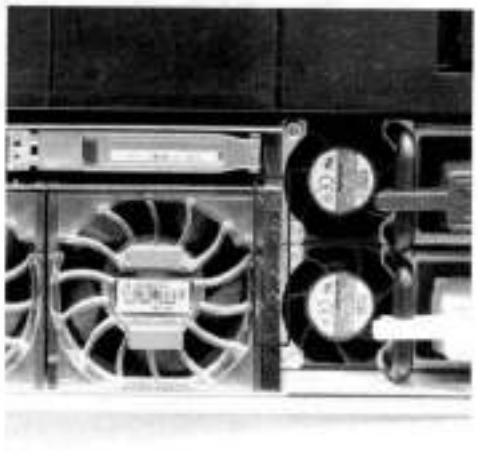


Figure 14. System LEDs

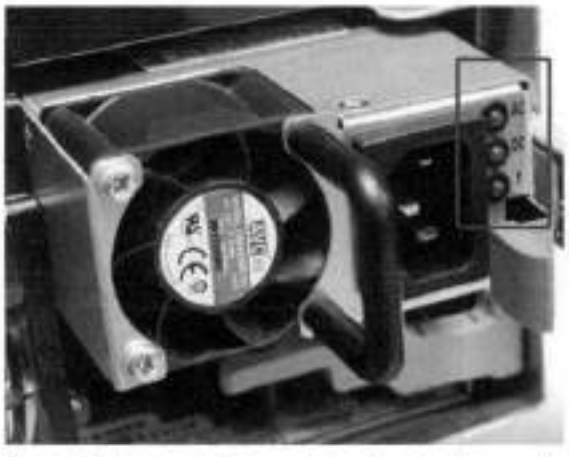
The next photo shows the location of the system LED legend label. Power supply LEDs shows the power supply LEDs. Other front LEDs are shown in Fan and SSD LEDs. LED states are described in LED status indicators.

Figure 15. System LED legend label

The power supply LEDs include:

- AC LED on top
- DC LED in the middle
- Failure LED on the bottom

Figure 16. Power supply LEDs



Each SSD has two LEDs as shown in the following figure. The lower left corner of the housing around each fan acts as an LED, glowing amber when the fan has failed.

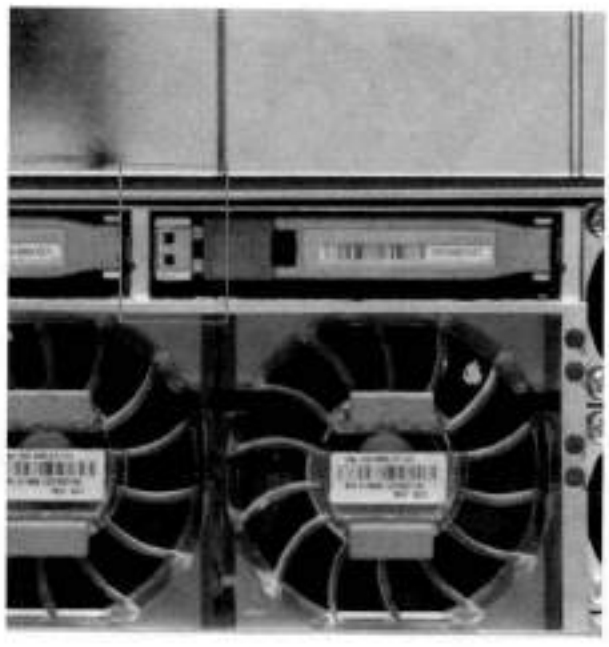


Figure 17. Fan and SSD LEDs

Table 16. LED status indicators

Part	Description or Location	State
System	Dot within a circle (top LED)	Blue indicates power on and normal operation.
System, SP fault	Exclamation point within a triangle	Dark indicates normal operation. Amber indicates failure.
System, chassis fault	Exclamation point within a triangle with a light below	Dark indicates normal operation. Yellow indicates a fault condition.
System	Marked out hand within a black square (bottom LED)	White warns not to remove the unit.
Power supply	AC LED	Steady green indicates normal AC power.
Power supply	DC LED	Steady green indicates normal DC power.
Power supply	Failure LED	Solid amber indicates a failed power supply.
SSD	Top LED	Solid blue, disk ready, blinks while busy.
SSD	Bottom LED	Dark indicates healthy. Solid amber indicates disk fail.
Fan	Fan housing	The fan housing glows an amber color during fan failure.

Back Panel

The photo shows the hardware features and interfaces on the back of the system.

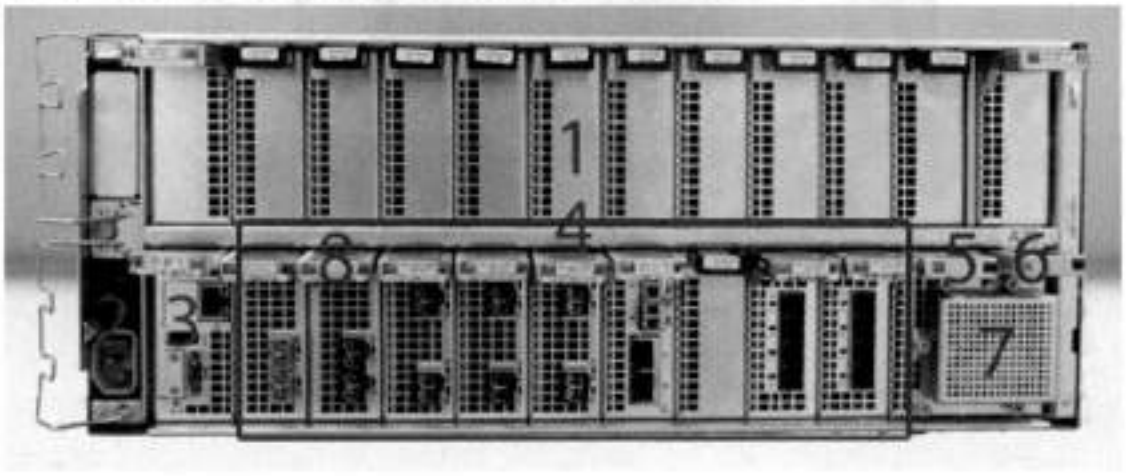


Figure 18. Features on rear of chassis

1. Upper level contains all blanks
2. AC power extender module
3. Management module (slot Mgmt A)
4. Red box indicating I/O modules (slots 0-8)
5. Battery backup (BBU in slot 9)
6. NVRAM module (slot 10)
7. Cage covering the BBU and NVRAM combination module
8. I/O LED at the end of each I/O module handle
9. Location of serial number label/tag

NOTE: For modules containing multiple ports, the bottom port is numbered as zero (0) with numbers increasing going upward.

I/O module LEDs

Each I/O module ejector handle contains a bi-colored LED. Green indicates normal function, while an amber color indicates a fault condition.

Management module and interfaces

The management module is on the left-most side when facing the back of the system, in slot Mgmt A. The process to remove and add a management module is the same as the I/O modules, however, the management module can only be accommodated in Mgmt A slot.

The management module contains one external LAN connection for management access to the SP module. One micro DB-9 connector is included to provide the console. A USB port is provided for use during service of the system to allow booting from a USB flash device.

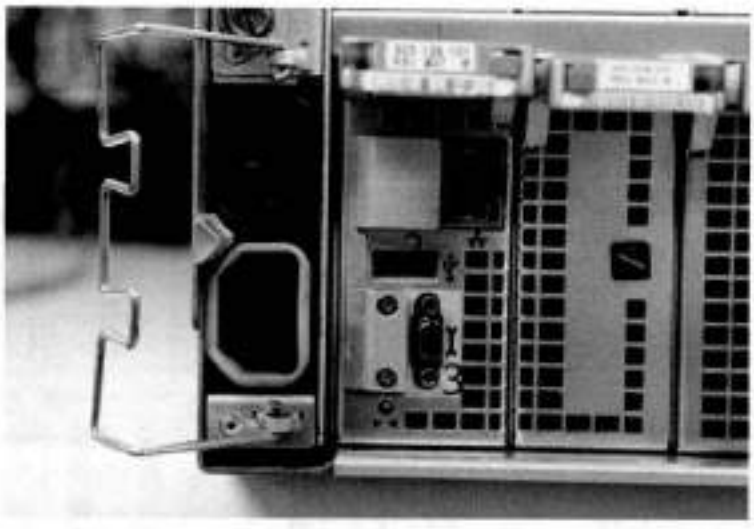


Figure 19. Interfaces on the management module

- 1 - Ethernet port
- 2 - USB port
- 3 - Micro serial port

I/O modules and slot assignments

The table shows the I/O module slot assignments for the systems. See Features on rear of chassis for a view of the slot positions on the back panel and Top view of SP module with SP cover removed for a top view.

Table 17. DD4200 slot assignments

Slot Number	DD4200	DD4200 with Extended Retention Software	DD4200 with DD Cloud Tier
MGMT A	Management module	Management module	Management module
0	Fibre Channel (FC), Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
1	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
2	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
3	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
4	Ethernet or empty	Ethernet or empty	Ethernet or empty
5	Ethernet or empty	SAS	Ethernet or empty
6	Empty	SAS	SAS
7	SAS	SAS	SAS
8	SAS	SAS	SAS
9	BBU	BBU	BBU
10	NVRAM	NVRAM	NVRAM

Slot addition rules

- A maximum of six optional I/O modules (FC plus Ethernet) are allowed in systems without Extended Retention software, and a maximum of five optional I/O modules (FC plus Ethernet) are allowed in systems with Extended Retention software.
- Additional FC modules should be installed in numerically increasing slot numbers immediately to the right of the existing FC modules, or starting in slot 0 if no FC modules were originally installed. A maximum of four FC modules are allowed in a system.
- Additional Ethernet modules should be installed in numerically decreasing slot numbers immediately to the left of the existing Ethernet modules or starting in slot 4 if no Ethernet modules were originally installed. For systems without Extended Retention software, a maximum of six (limited to four of any one type) Ethernet modules can be present. For systems with Extended Retention software, a maximum of five (limited to four of any one type) Ethernet modules can be present.
- All systems include two SAS modules in slots 7 and 8. Systems with Extended Retention software must have two additional SAS modules in slots 5 and 6.
- For systems without Extended Retention software, if adding I/O modules results in the allowed maximum of six I/O modules present, slot 5 is used. Slot 5 is only used for an Ethernet module. Adding FC modules in this specific case require moving an existing Ethernet module to slot 5. Other than this specific case, it is not recommended to move I/O modules between slots.
- Adding Extended Retention software to a system includes adding two SAS modules in slots 5 and 6. If the system originally had the maximum of 6 optional I/O modules, the I/O module in slot 5 must be permanently removed from the system.

Fibre Channel (FC) I/O Module Option

An FC I/O module is a dual-port Fibre Channel module. The optional virtual tape library (VTL) feature requires at least one FC I/O module. Boost over Fiber Channel is optional and the total FC HBAs cannot exceed more than allowable Fibre Channel cards per controller.

Ethernet I/O Module Options

The available Ethernet I/O modules are:

- Dual Port 10GBase-SR Optical with LC connectors

- Dual Port 10GBase-CX1 Direct Attach Copper with SPF+ module
- Quad Port 1000Base-T Copper with RJ-45 connectors
- Quad port 2 port 1000Base-T Copper (RJ45) /2 port 1000Base-SR Optical

Internal system components

The photo shows the system with the system processor (SP) module that is removed from the chassis and the SP cover removed.

Figure 20. Top view of SP module with SP cover removed

- 1 - Front of system
- 2 - Four groups of 4 DIMM cards

DIMM modules

DD4200 systems contain 16 x 8 GB of memory DIMM.

DD4200 and ES30 shelf guidelines

The Data Domain system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your Data Domain system as listed in the following table below.
- Use the Installation and Setup Guide for your Data Domain system to minimize the chance of a cabling mistake.
- A Data Domain system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.
- ES30 SATA shelves must be on their own chain.

NOTE:

- ES30 SAS shelves must be running DD OS 5.4 or later.
- ES30-45 SATA shelves must be running DD OS 5.4 or later.
- DD OS 5.7 and later support 4TB drives.

Table 18. DD4200 and ES30 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	ES30 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB) [1]	Max RAW external capacity (TB) [2]
DD4200[3]	128	2x4	SAS 30, 45; SATA 15, 30, 45[5]	5[6]	4	192	256
DD4200 ER [3, 4]	128	4x4	SAS 30, 45; SATA 15, 30, 45[5]	7	8	384	512
DD4200 w/ DD Cloud Tier	128	3x4	SAS 30, 45; SATA 15, 30, 45[5]	7	8	192 (max), additional 72 SAS dedicated to DD Cloud Tier	256 (max), additional 90 SAS dedicated to DD Cloud Tier

1. This figure only counts drives that have user data in the shelves.

2. The raw capacity of an ES30 is 125% of the available capacity.

3. The maximum shelf count for any specific drive/shelf size might be less than the product of max shelves x max shelves per set.

4. With Extended Retention software.

5. ES30-45 (SATA) is only supported with DD OS 5.4 or later.

6. 5 shelves maximum with ES30, 4 is the recommended maximum.

Types of cabinets and power connections

The ES30 chassis is installed in two types of racks: 40U-C (existing racks) and the 40U-P (newer racks). The racks use one phase or 3-phase power connections.

This section describes the different types of racks and the power connections for the ES30 chassis.

Single phase power connections for 40U-P (current racks)

The following illustrations show single phase power connections for 40U-P racks that are used for several Data Domain systems.

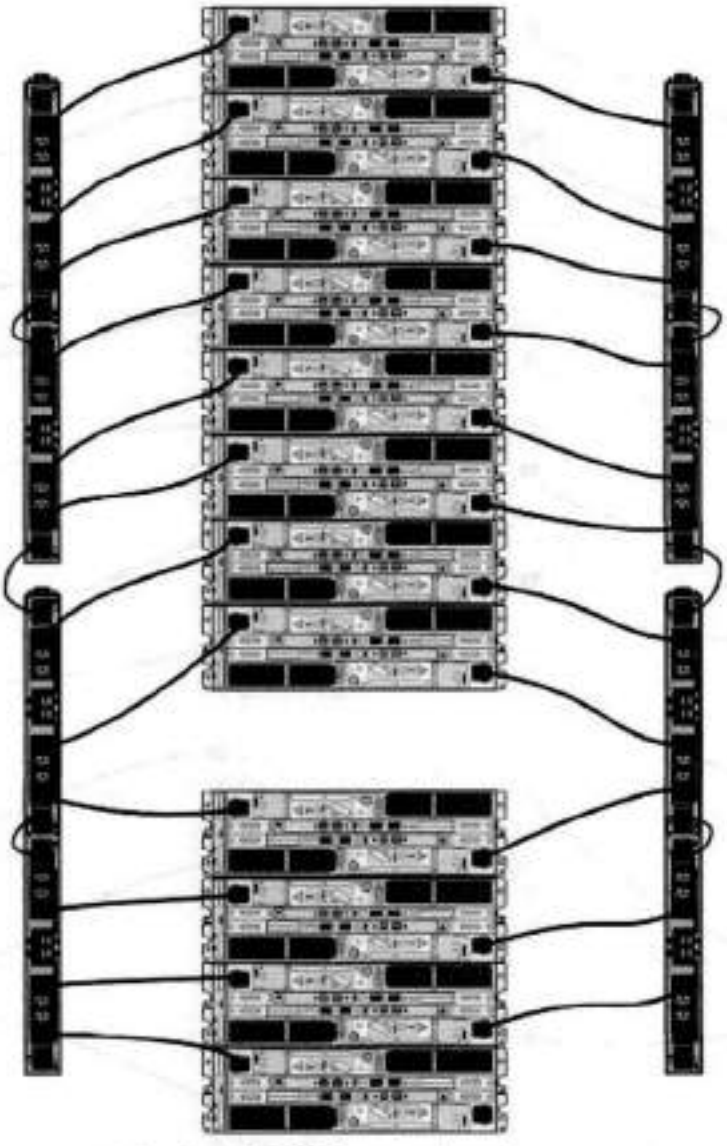


Figure 21. Single phase power connections for the 40U-P expansion rack

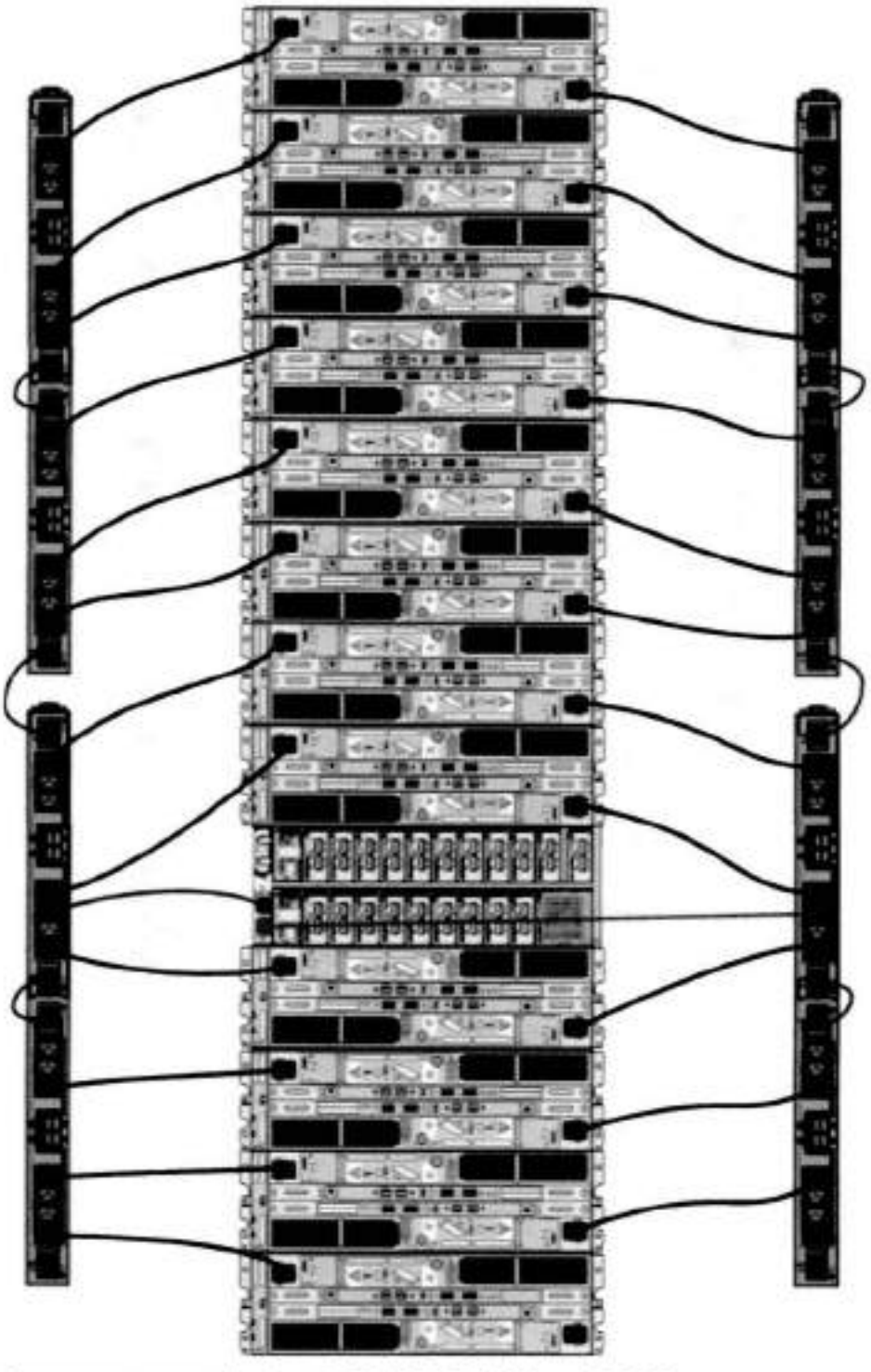


Figure 22. Single phase power connections for the DD4200, DD4500, and DD7200

Single phase power connections for 40U-C (older racks)

The following illustrations show single phase power connections for 40U-C racks that are used for several Data Domain systems.

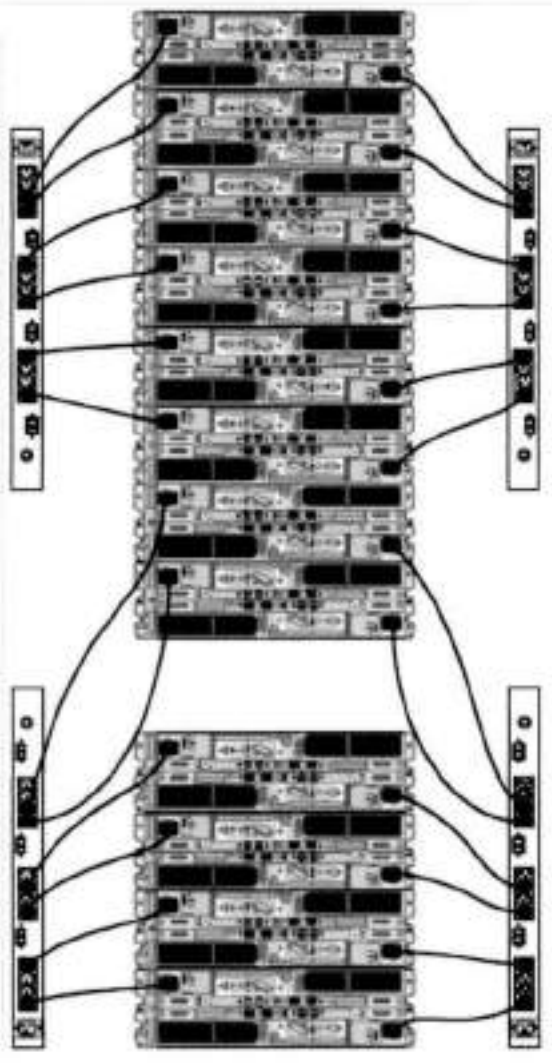


Figure 23. Single phase power connections for the Expansion Rack

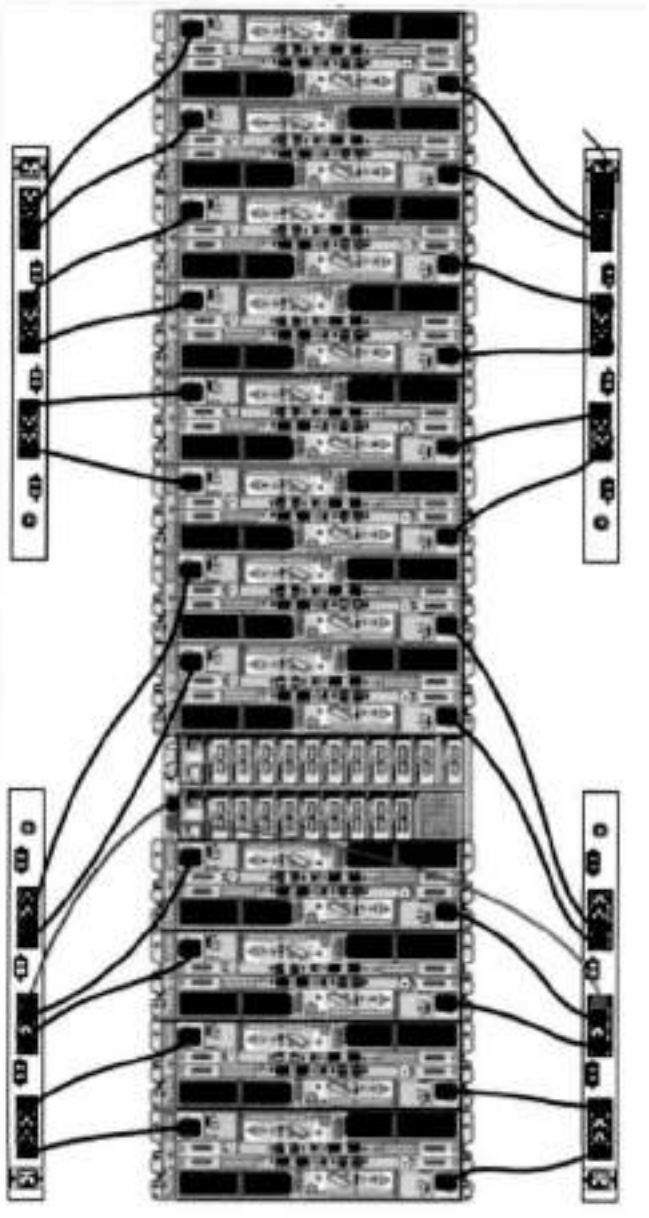


Figure 24. Single phase power connections for the DD4200, DD4500, and DD7200

3-Phase power connections for 40U-C (older racks)

The following illustrations show single phase power connections for 40U-C racks that are used for several Data Domain systems.

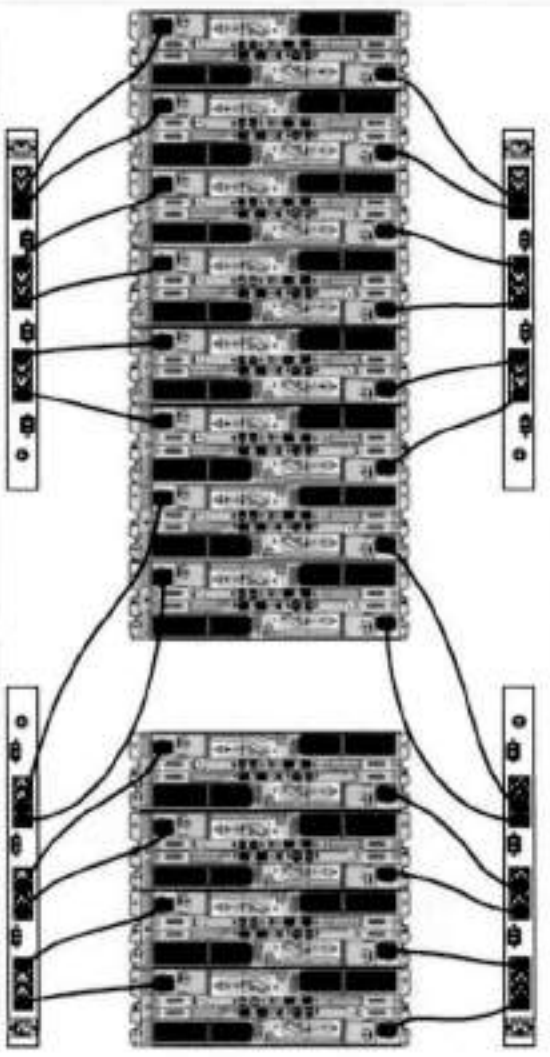


Figure 25. Single phase power connections for the Expansion Rack

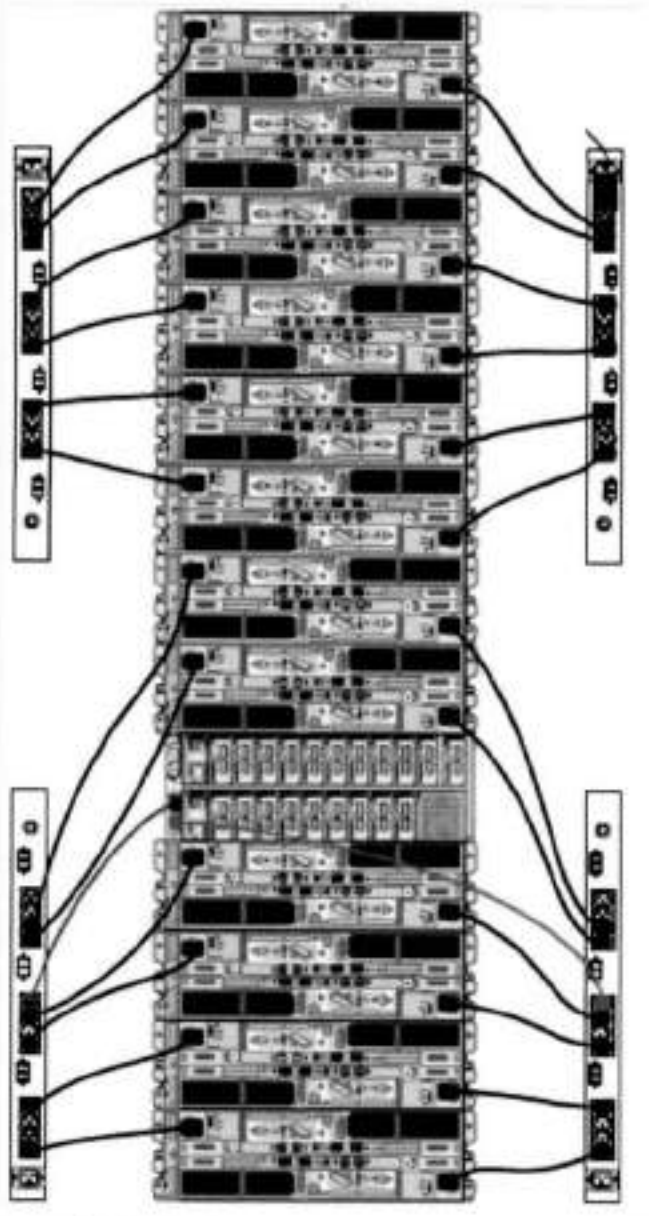


Figure 26. Single phase power connections for the DD4200, DD4500, and DD7200

3-Phase power connections for 40U-P (current racks)

Some environments use 3-phase power for 40U-P racks that are used for several Data Domain systems. In those situations, it is desirable to balance the current draw across all three phases. The recommended 3-phase power cabling attempts to do that, but an optimal configuration depends on the specific installation. The following illustrations show recommended 3-phase power connections for several Data Domain systems.

NOTE: The next few diagrams show recommended 3-phase delta power connections.

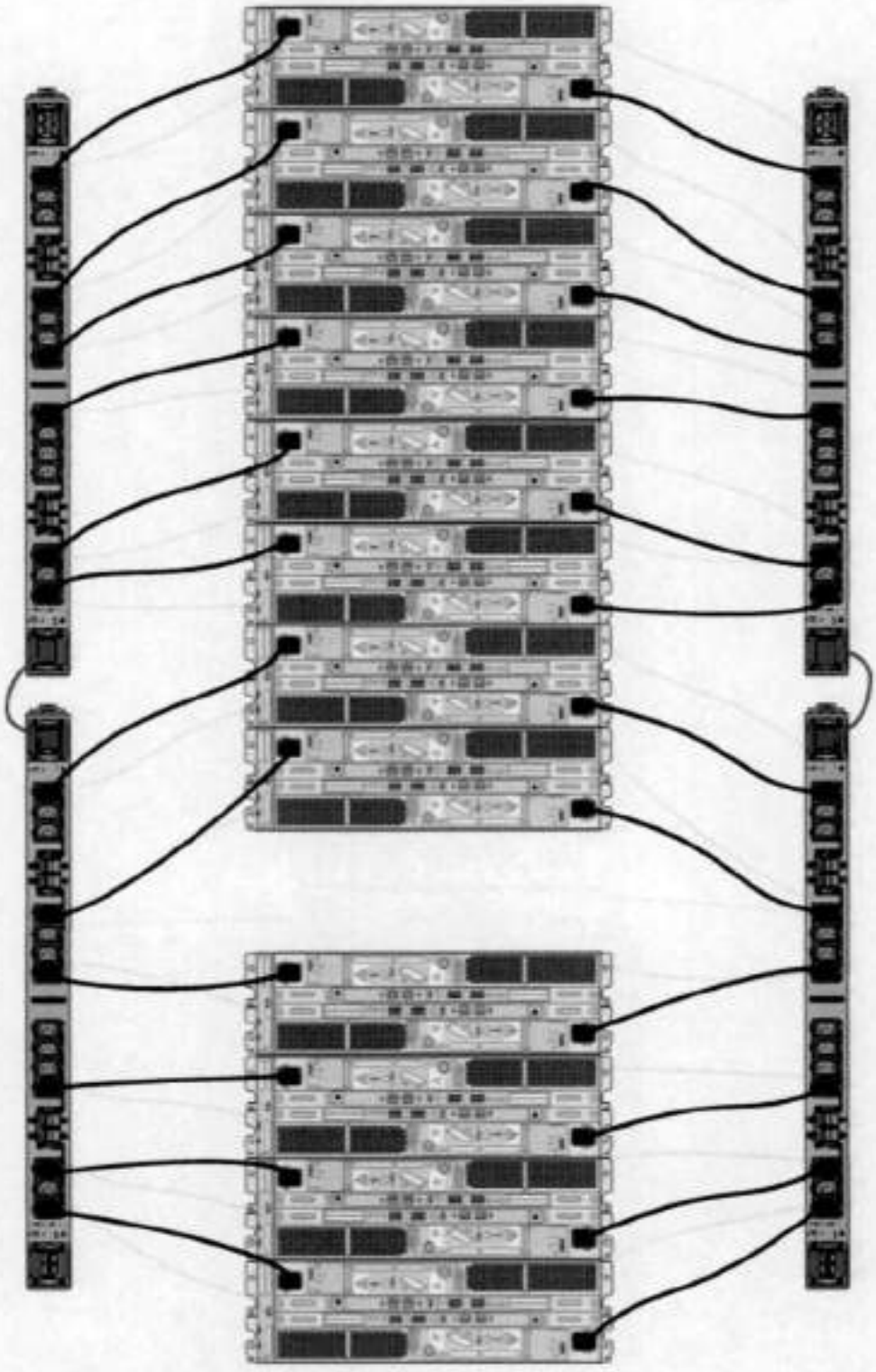


Figure 27. Recommended 3-phase delta power connections for the Expansion Rack

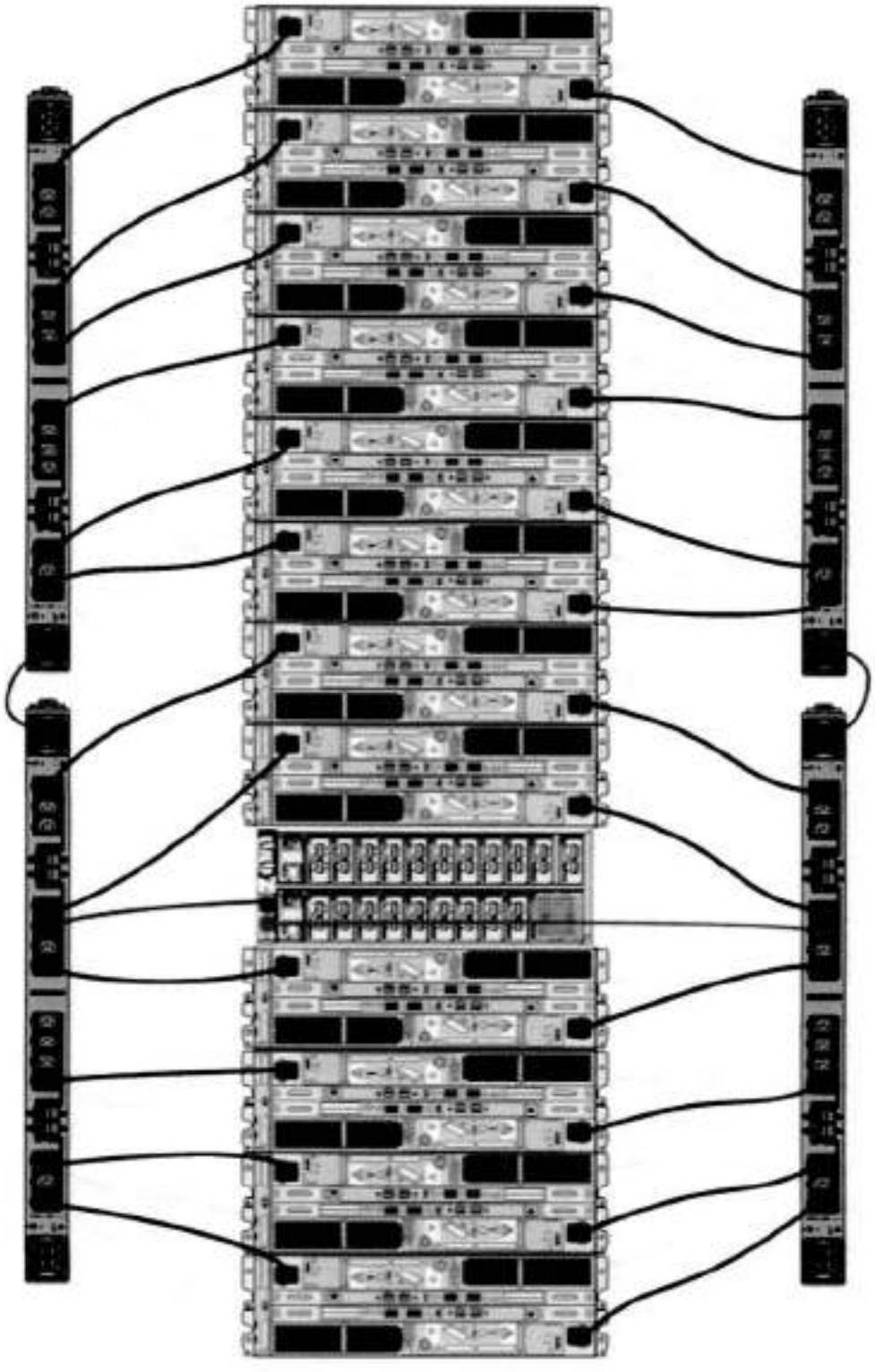


Figure 28. Recommended 3-phase delta power connections for DD4200, DD4500, and DD7200

NOTE: The next few diagrams show recommended 3-phase wye power connections.

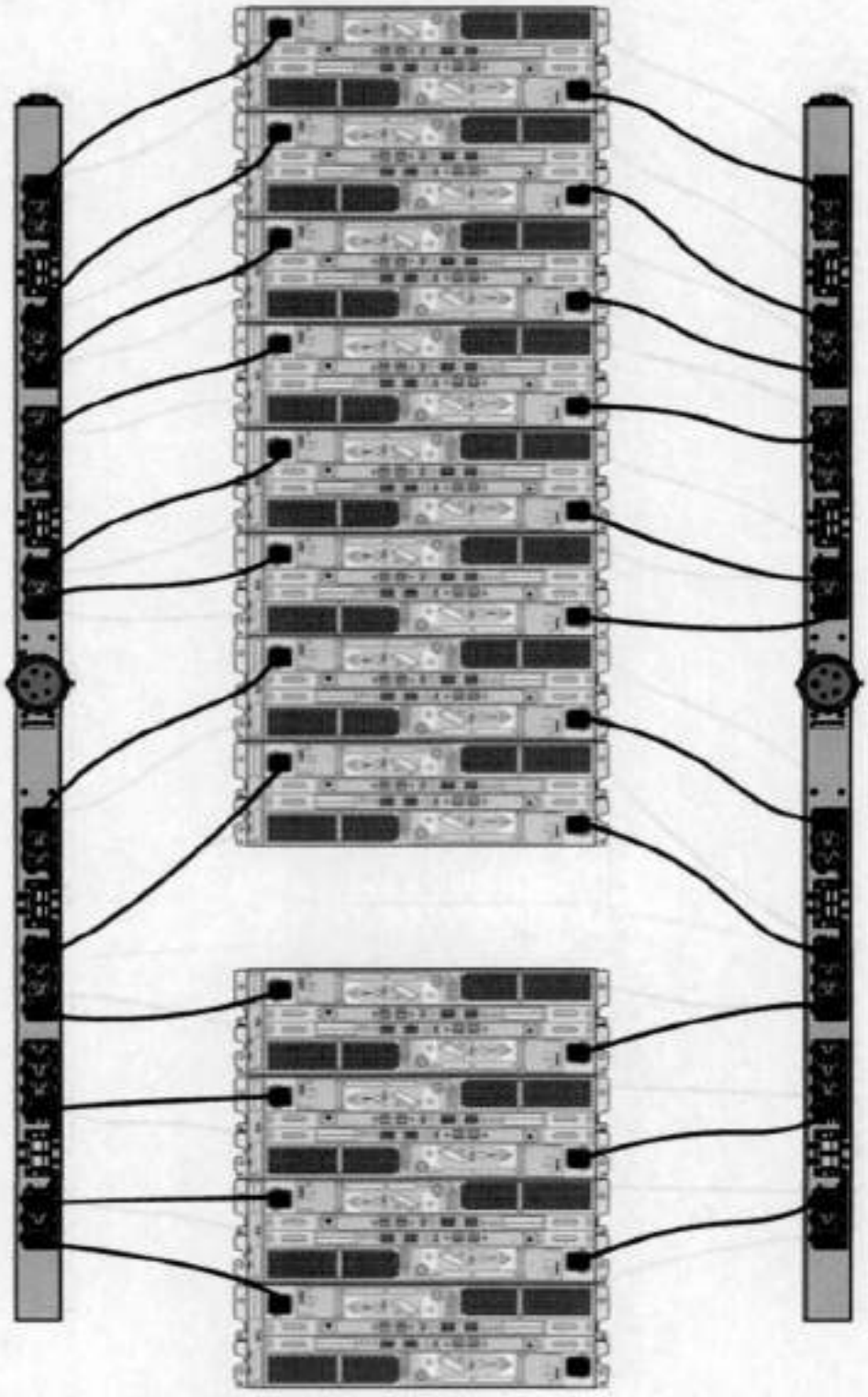


Figure 29. Recommended 3-phase wye power connections for the Expansion Rack

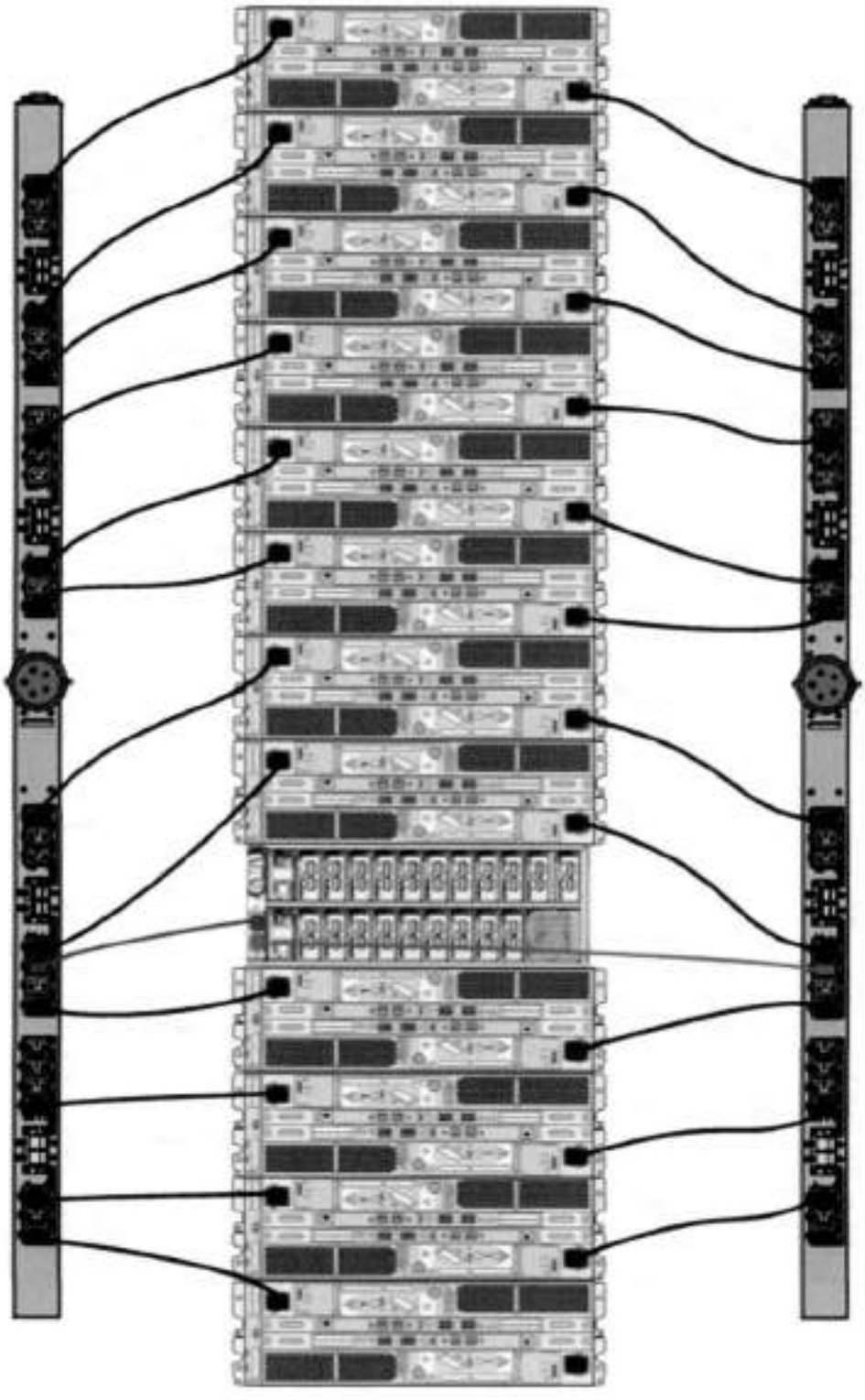


Figure 30. 3-phase wye power connections for DD4200, DD4500, and DD7200

Cabling shelves

NOTE:

- Before cabling the shelves, physically install all shelves in the racks. Refer to the rail kit installation instructions included with the ES30 shelf for rack mounting.

- The documentation refers to two SAS HBAs. If only one HBA is allowed in a system, then use another port as defined later for that specific system.
- On an HA system, add cables from the second node to open ports at the end of the sets. The ports on the second node must connect to the same sets as the corresponding ports on the first node.

Ports on the system's SAS HBA cards connect directly to a shelf controller's host port. For redundancy, you need to create dual paths by using a port on one SAS HBA card to connect to one shelf controller in each shelf set, and a port on another SAS HBA card to connect to another shelf controller in the same shelf set. With dual paths, if one SAS HBA card fails, the shelf is still operational. However, in the unlikely event any single shelf becomes completely disconnected from power or SAS cables and becomes disconnected from a previously operational shelf, the file system goes down and the shelf is not operational. This is considered a double failure.

There are two kinds of configurations: one shelf in a set or multiple shelves in a set.

ES30 and DD4200 cabling

There are a few rules that must be followed when adding a mixture of ES20, ES30 SATA, and ES30 SAS shelves to your system. If a system does not follow ALL of these rules it is not a legitimate configuration.

Prerequisites:

- Follow the minimum and maximum shelf capacity configuration provided in the table.
- You cannot have ES20 and ES30 shelves in the same set.
- You cannot have ES30 SATA and ES30 SAS shelves in the same set.
- You cannot exceed the maximum amount of raw capacity displayed in the product's cabling table.
- The maximum number of shelves displayed in the product's cabling table cannot be exceeded.
- You cannot have more than four ES20s in a single set (maximum preference is three).
- You cannot have more than five ES30s in a single set (maximum preference is four).
- You can have a maximum of seven ES30s for systems with Extended Retention software.
- There are no specific placement or cabling requirements for the metadata shelves for DD Cloud Tier configurations. These shelves can be installed and cabled the same way as standard ES30 shelves.

NOTE: An ES20 requires more power than an ES30. Ensure that your rack is configured to handle the power needs.

The tables below show how to configure a mixed system. To use the tables, go to the appropriate system. Then find the number of ES20s that are to be configured in the first column. The next column defines the number of ES20 sets. If there are multiple rows with the same number of ES20s then pick the row with the appropriate number of ES20 SATA shelves. The next column in that row defines the number of sets of ES30 SATA shelves. Finally, there may be entries for the number of desired ES30 SAS shelves and the number of sets to be used.

If the combinations of shelves exceed the supported usable storage, there may not be an entry. The entries are based on the smallest usable storage per shelf type (12TB for ES20, 12 TB for ES30 SATA, and 24TB for ES30 SAS). Always check that the sum of the usable storage of all of the shelves does not exceed the supported usable storage of the configuration.

Table 19. Minimum and maximum configurations

System	Minimum appliance shelf count	Maximum appliance shelf count	DD Cloud Tier systems in TB	Extended Retention systems (ER) in TB	Max shelves for ER
4200 (192)	1	16	• 189 • 90 for metadata	• DD OS 5.4 and earlier: 576 • DD OS 5.5 and later: 385	32

Systems without Extended Retention or DD Cloud Tier all support four chains. The following tables show combinations of ES20 and ES30 shelves. For combinations of any two types of shelves, these tables can be used as a guide.

Table 20. DD4200 cabling information

DD4200					
ES20	ES20 chains	ES30 SATA	ES30 SATA chains	ES30 SAS	ES30 SAS chains
13-16	4	0	0	0	0
9-12	3	1-5	1	0	0

Table 20. DD4200 cabling information (continued)

DD4200					
9-12	3	0	0	1-3	1
5-8	2	6-10	2	0	0
5-8	2	1-5	1	1-5	1
5-8	2	0	0	5	2
5-8	2	0	0	1-4	1
1-4	1	8-12	3	0	0
1-4	1	6-10	2	1-5	1
1-4	1	1-5	1	1-4	1
1-4	1	1-5	1	5-7	2
1-4	1	0	0	1-4	1
1-4	1	0	0	5-7	2
0	0	13-16	4	0	0
0	0	9-12	3	1-3	1
0	0	5-8	2	1-4	1
0	0	5-8	2	5	2
0	0	1-4	1	1-4	1
0	0	1-4	1	5-7	2
0	0	0	0	1-4	1
0	0	0	0	5-8	2

The following figures show cabling for base systems, systems with the Extended Retention software option, and systems integrated with an Avamar system.

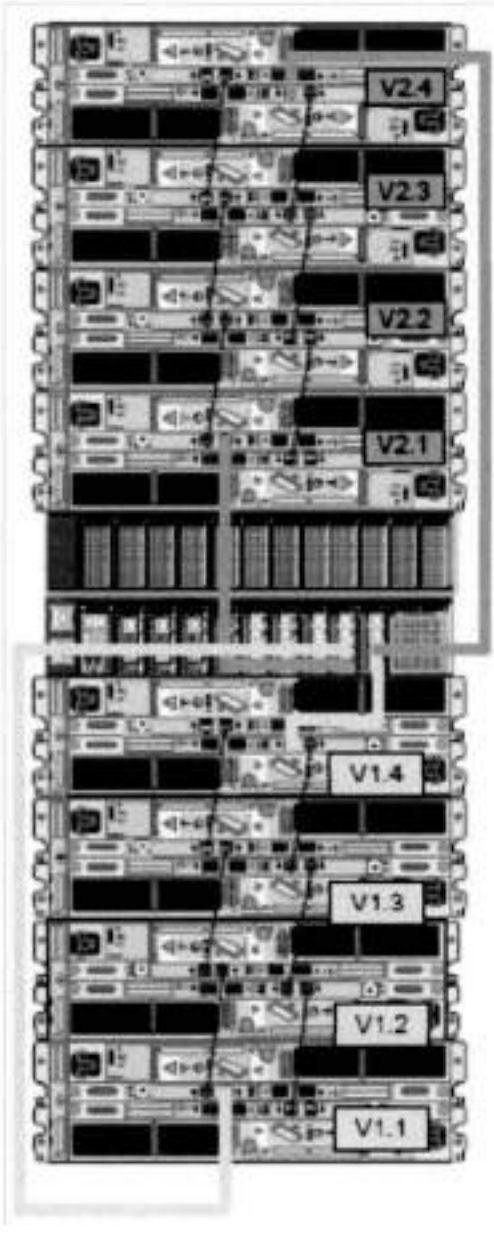


Figure 31. Recommended DD4200 cabling

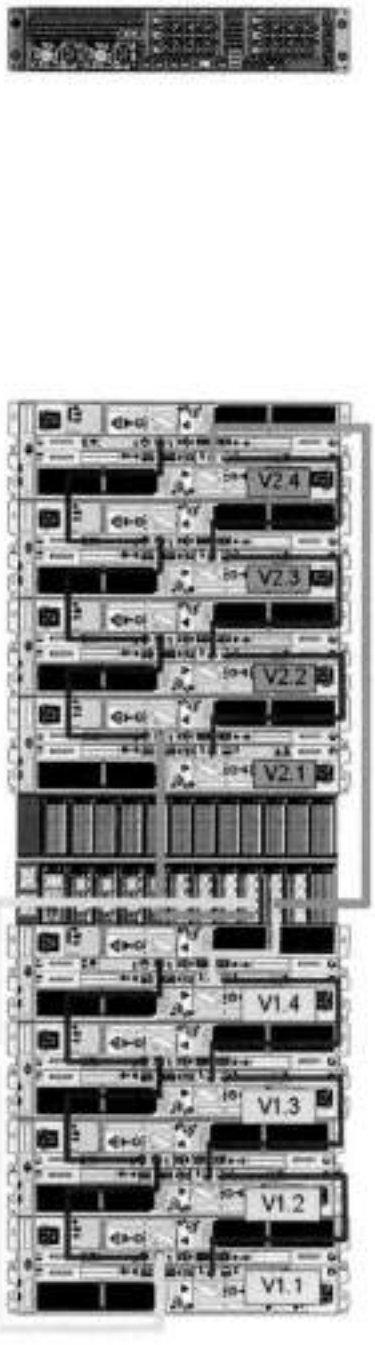


Figure 32. Recommended cabling for DD4200 integrated with Avamar

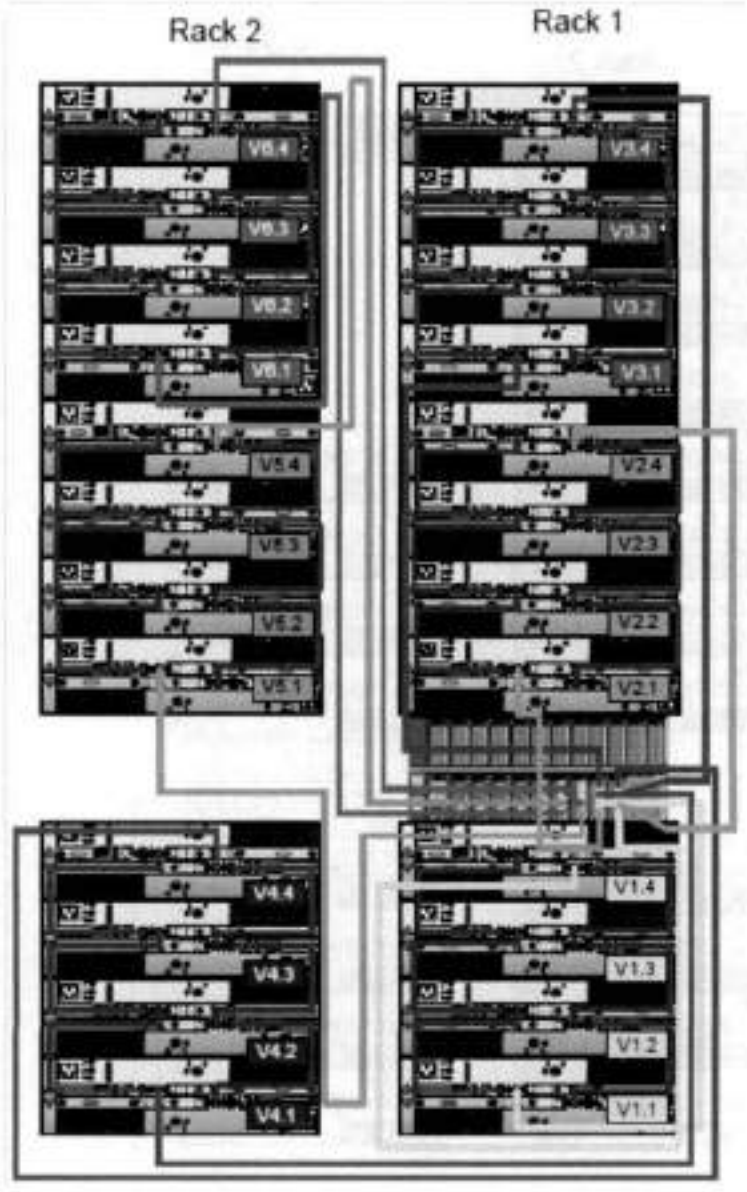


Figure 33. Recommended cabling for DD4200 system with extended retention software or DD Cloud Tier

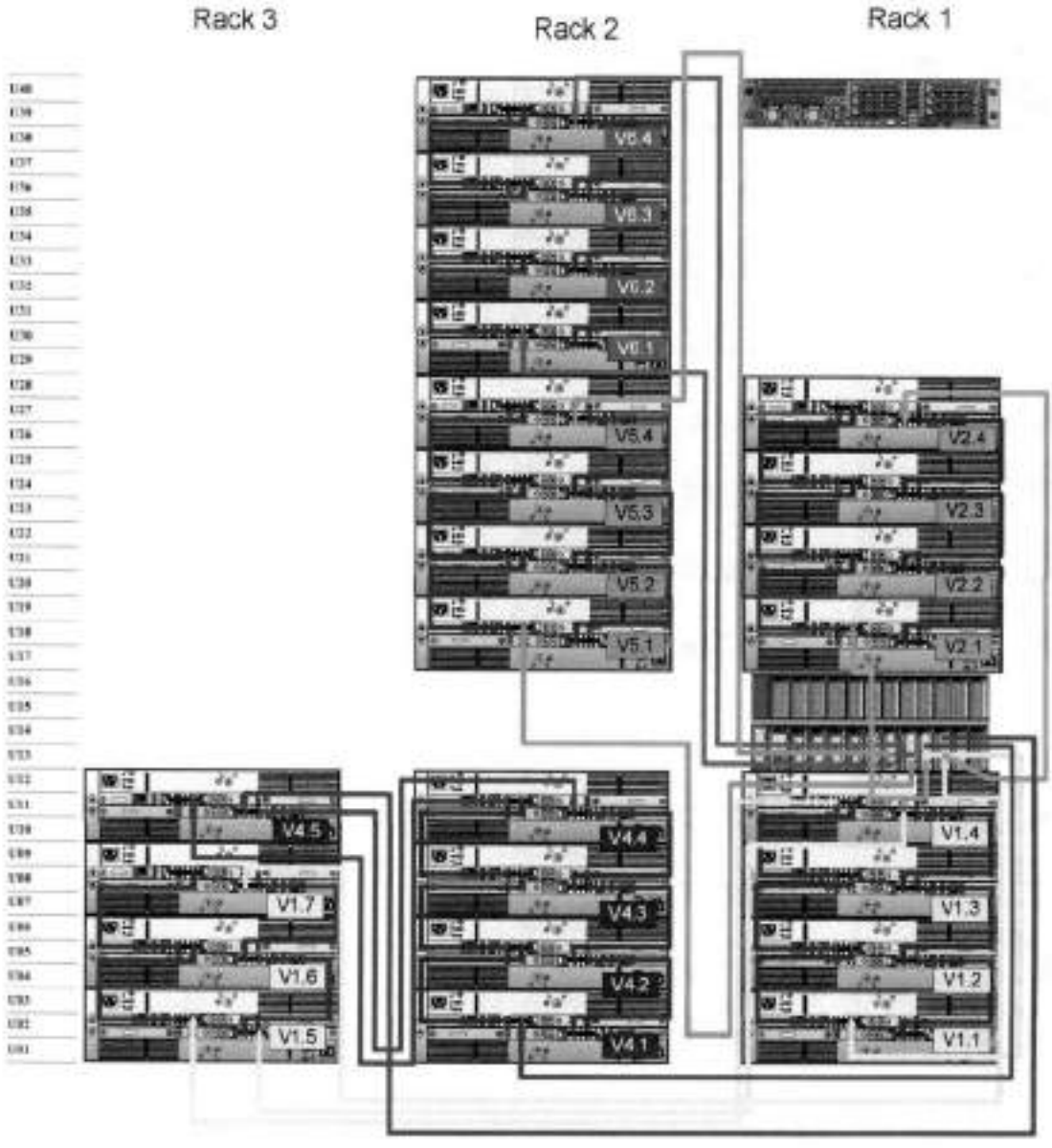


Figure 34. Recommended cabling for DD4200 with extended retention and integrated with Avamar

DD4200 and DS60 shelf guidelines

The Data Domain system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your Data Domain system as listed in the following table.
- For redundancy, the two connections from a Data Domain system to a set of shelves must use ports on different SAS I/O modules.
- Use the Installation and Setup Guide for your Data Domain system to minimize the chance of a cabling mistake.
- A Data Domain system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.
- ES30 SATA shelves must be on their own chain.
- If ES30 SAS shelves are on the same chain as a DS60, the maximum number of shelves on that chain is 5.

- DD OS 5.7.1 does not support HA with SATA drives.

Table 21. DD4200 and DS60 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	DS60 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB)[1]	Max RAW external capacity (TB)
DD4200	128	2x4	SAS 45	1	4	192	240
DD4200 ER [2]	128	4x4	SAS 45	2	8	384	480

NOTE: An entry of 45 corresponds to DS60-3 models and an entry of 60 corresponds to DS60-4 models.

1. This column only counts drives that have user data in the shelves. For example, a DS60 4-240 has 192TB.

2. With Extended Retention software.

Single phase power connections for 40U-P (current racks)

The following figures show single phase power connections for several Data Domain systems.

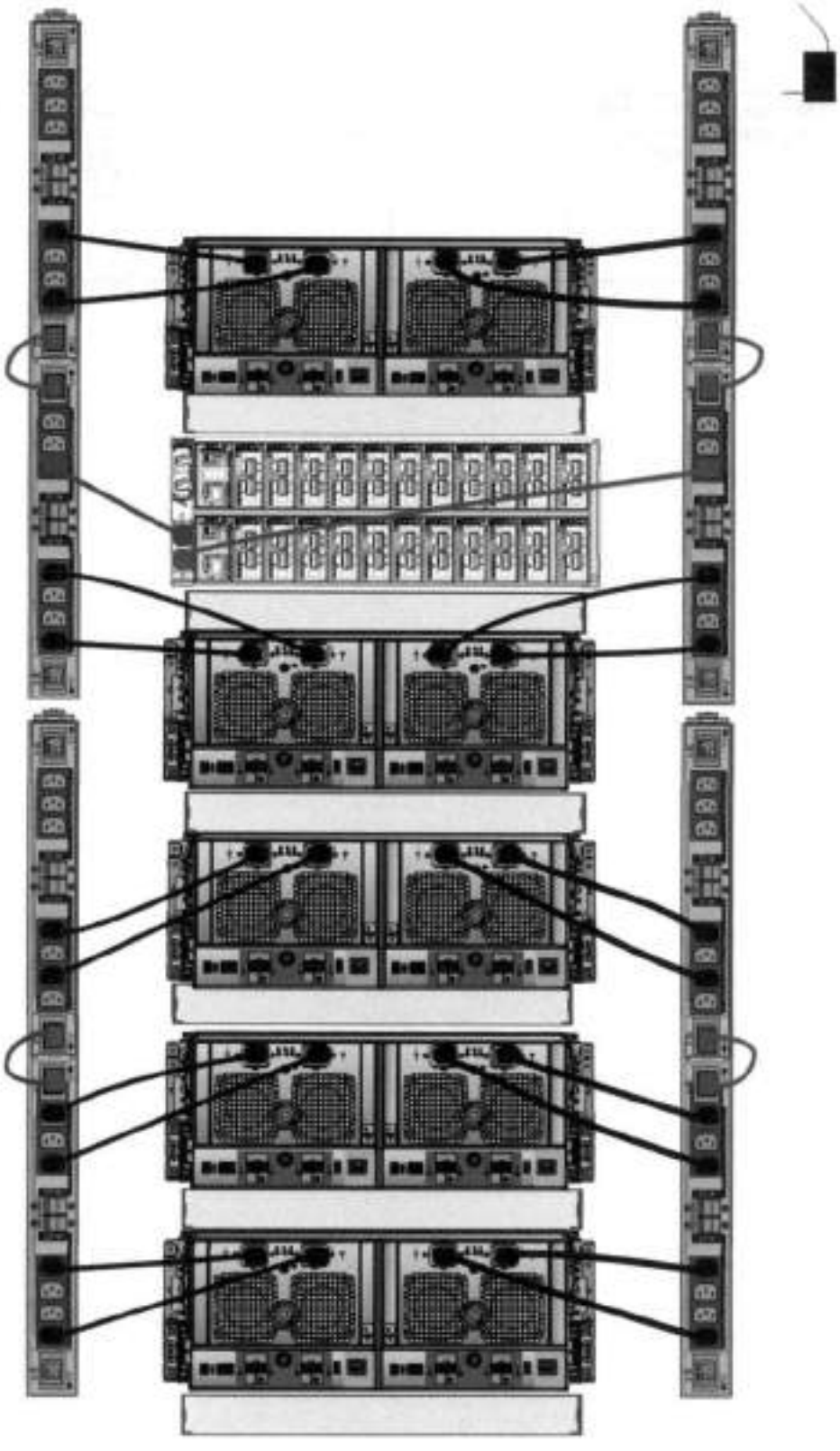


Figure 35. Single phase power connections for DD4200, DD4500, and DD7200 systems

3-phase power connections for 40U-P (current racks)

Some environments use 3-phase power for 40U-P racks used for several Data Domain systems. In those situations it is desirable to balance the current draw across all 3 phases. The recommended 3-phase power cabling attempts to do that, but an optimal

configuration is dependent on the specific installation. The following figures show recommended 3-phase power connections for several Data Domain systems.

NOTE: The next few diagrams show recommended 3-phase delta power connections.

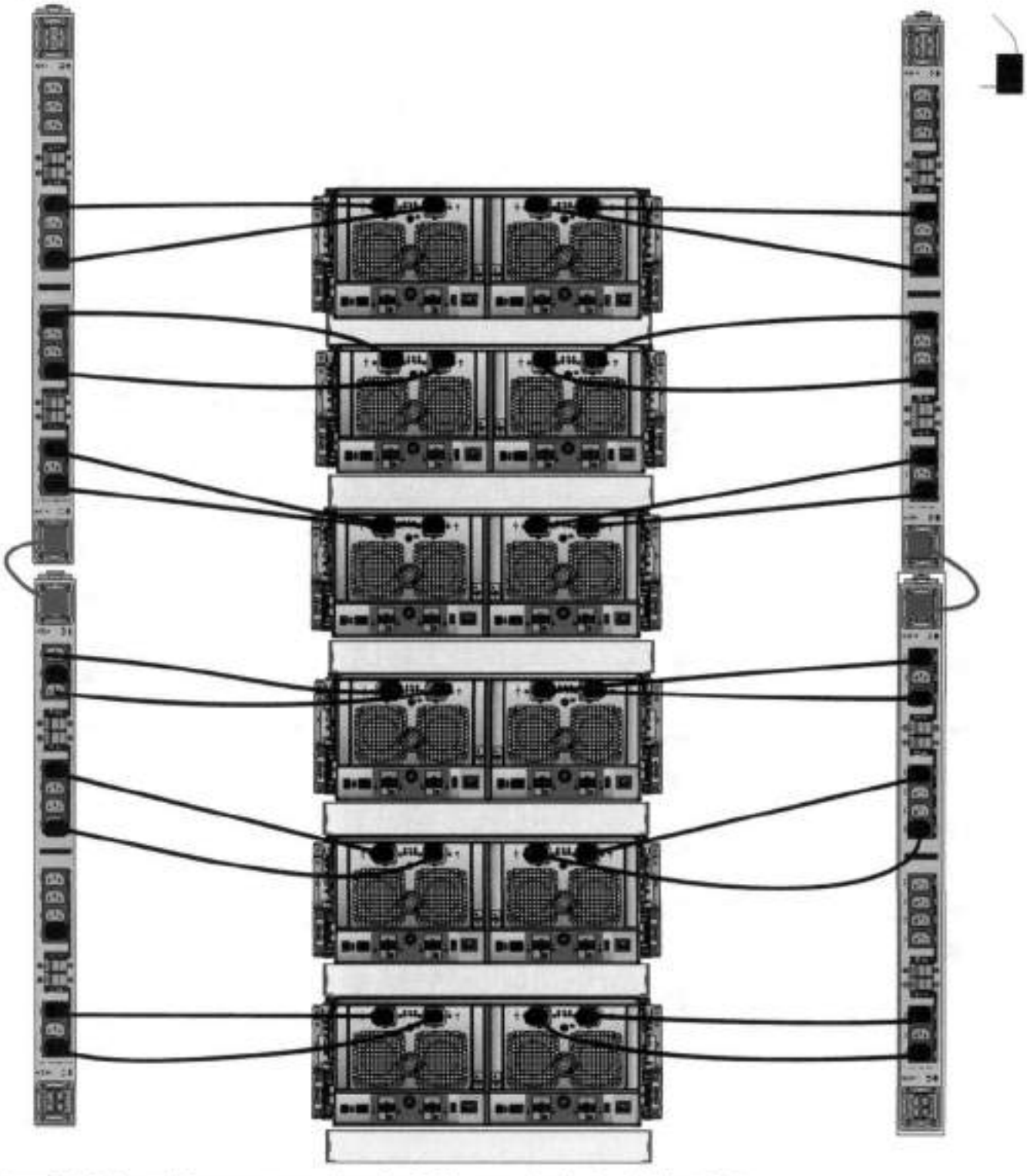


Figure 36. 3-phase delta power connections for DS60 expansion shelves (full-racked)

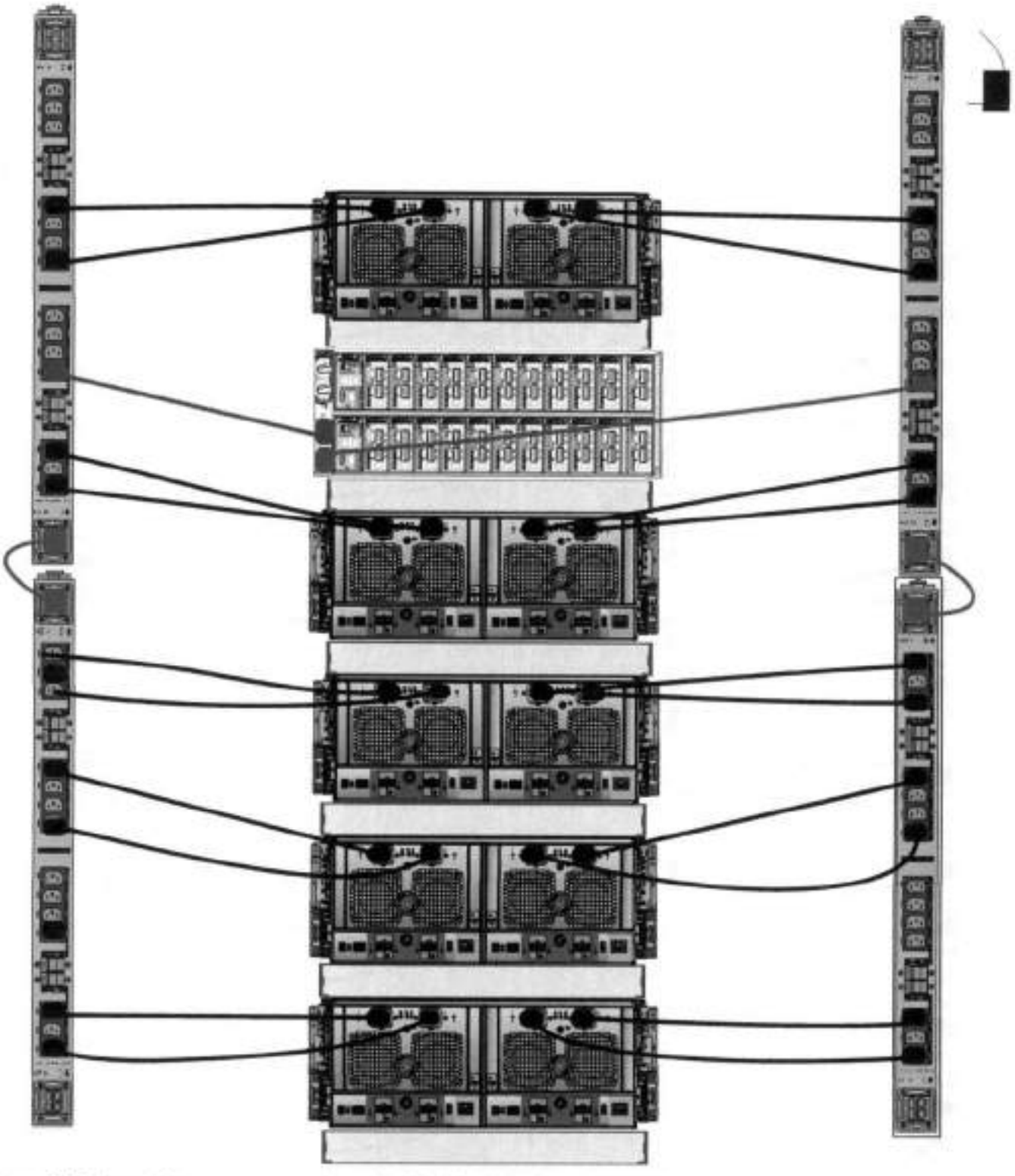


Figure 37. 3-phase delta power connections for DD4200, DD4500, and DD7200 systems

NOTE: The next few diagrams show recommended 3-phase wye power connections.

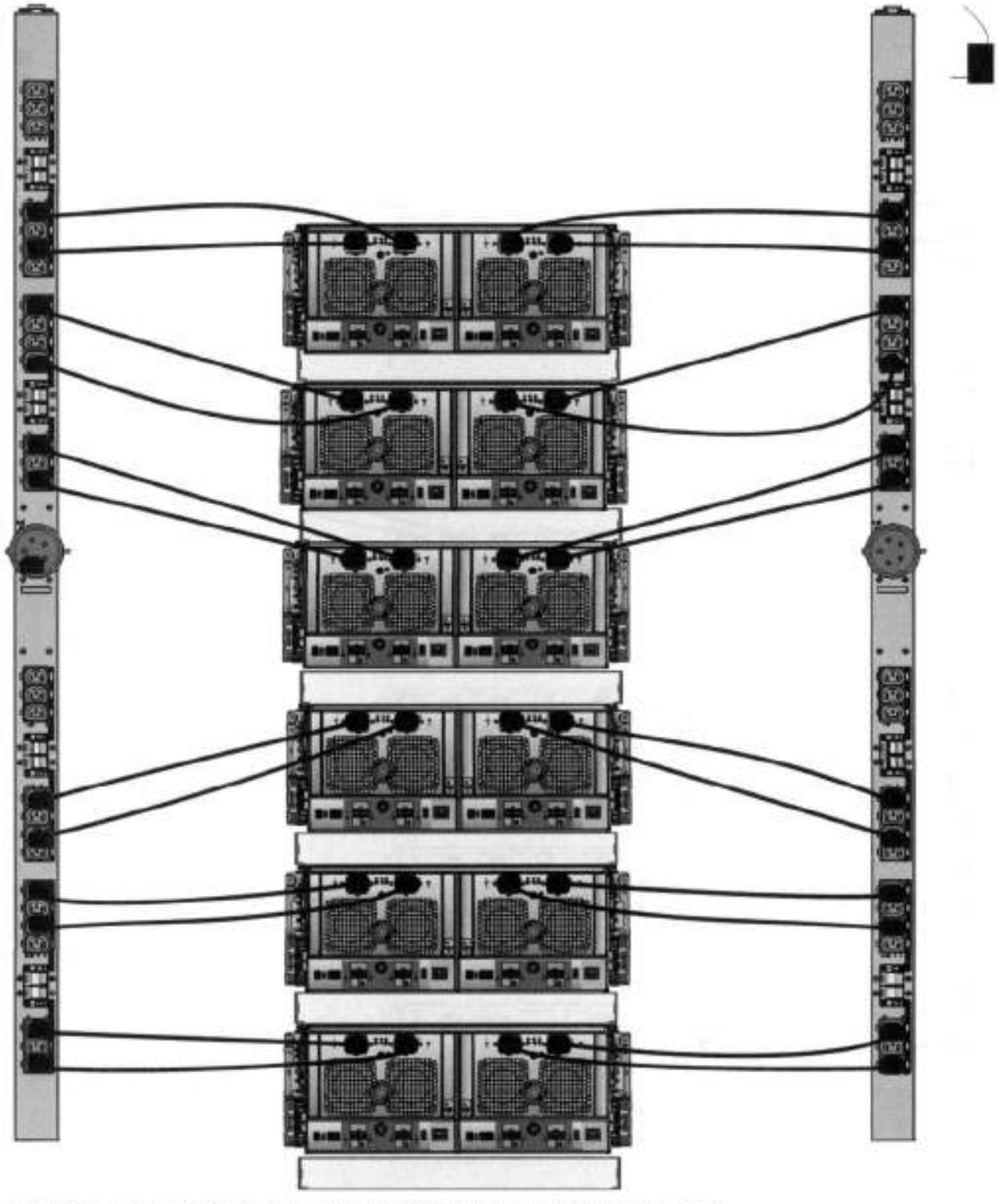


Figure 38. 3-phase wye power connections for DS60 expansion shelves (full-racked)

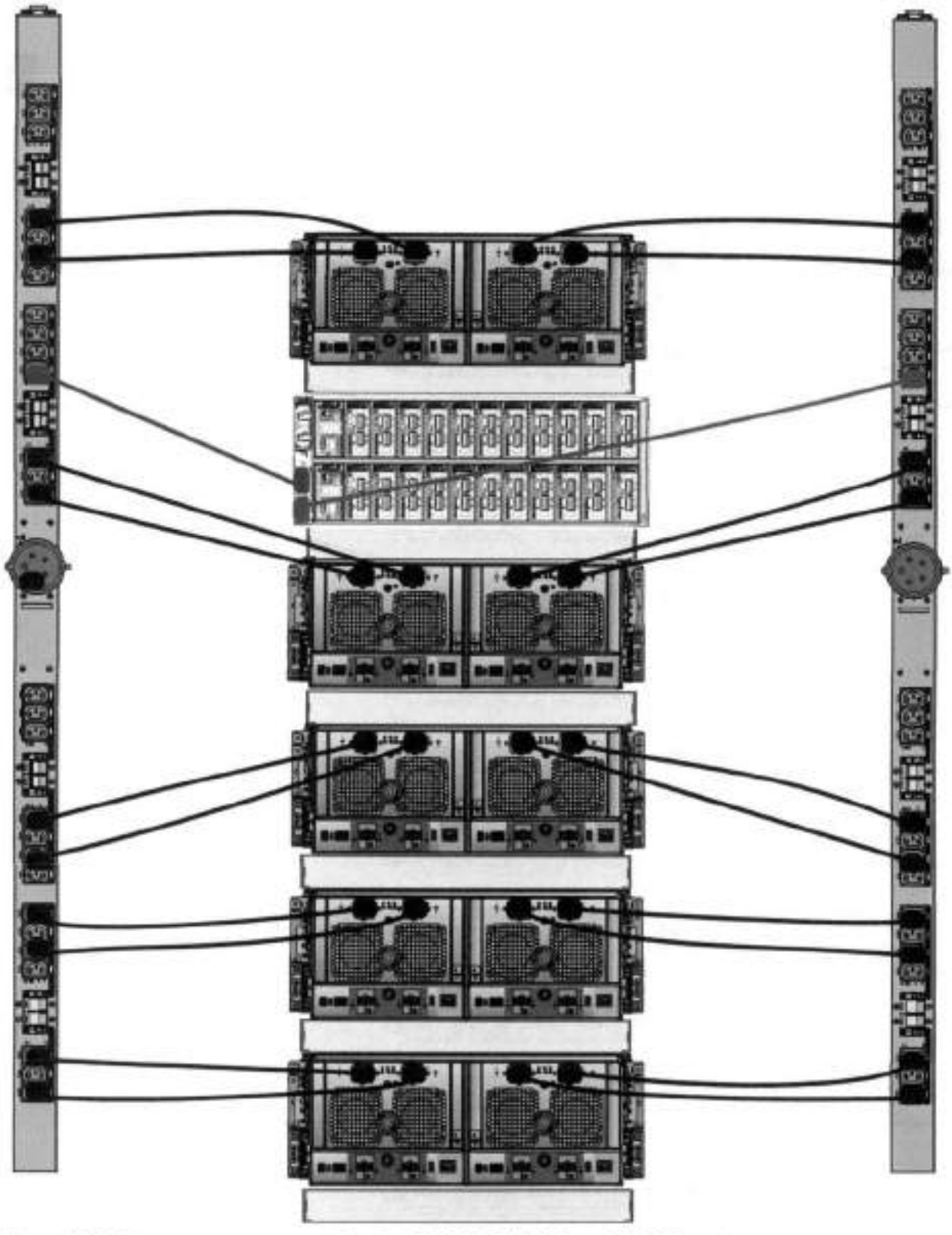


Figure 39. 3-phase wye power connections for DD4200, DD4500, and DD7200 systems

DS60 and DD4200 cabling

There are a few rules that must be followed when adding a mixture of DS60 and other shelf types to your system.

CAUTION: **If a system does not follow all these rules, it is not a legitimate configuration.**

Prerequisites:

- You cannot exceed the maximum amount of usable capacity displayed in cabling table for each system.
- You cannot exceed the maximum number of shelves displayed in cabling table for each system.
- You cannot connect more than two DS60 shelves in a single set.

Table 22. Minimum and maximum configurations

System	Appliance maximum	Minimum appliance shelf count
DD4200	192 TB	1

Mixing DS60, ES30, and ES20 shelves:

The non-Extended Retention versions of these systems all support four chains.

Extra planning and reconfiguration may be required to add DS60 shelves to system with ES20 shelves, ES30 SATA shelves, or a combination of shelves.

- The ES20 shelves must be on their own set. Minimize the ES20 set count by combining up to four ES20s per set.
- ES30 SATA shelves must also be on their own sets. Minimize the ES30 set count by combining up to five ES30s per set. If required, combine up to seven ES30 SAS shelves per set to minimize the set count.
- A set can contain a maximum of two DS60 shelves and, if required because of other restrictions, add ES30 SAS shelves up to a maximum of five shelves in that set.

NOTE: The configuration rules apply also to Extended Retention systems.

The following figures show cabling for base systems and systems with the Extended Retention software.

NOTE: It is recommended that the DS60 shelf with the greater number of drives should always be placed in the bottom position.

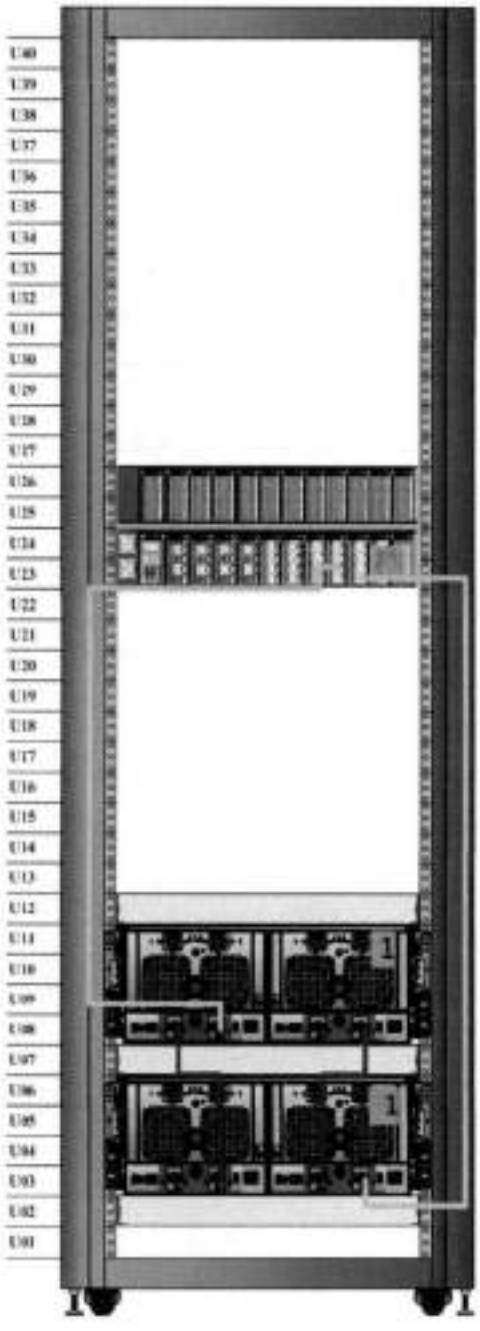


Figure 40. Recommended cabling for DD4200 (3TB drives)

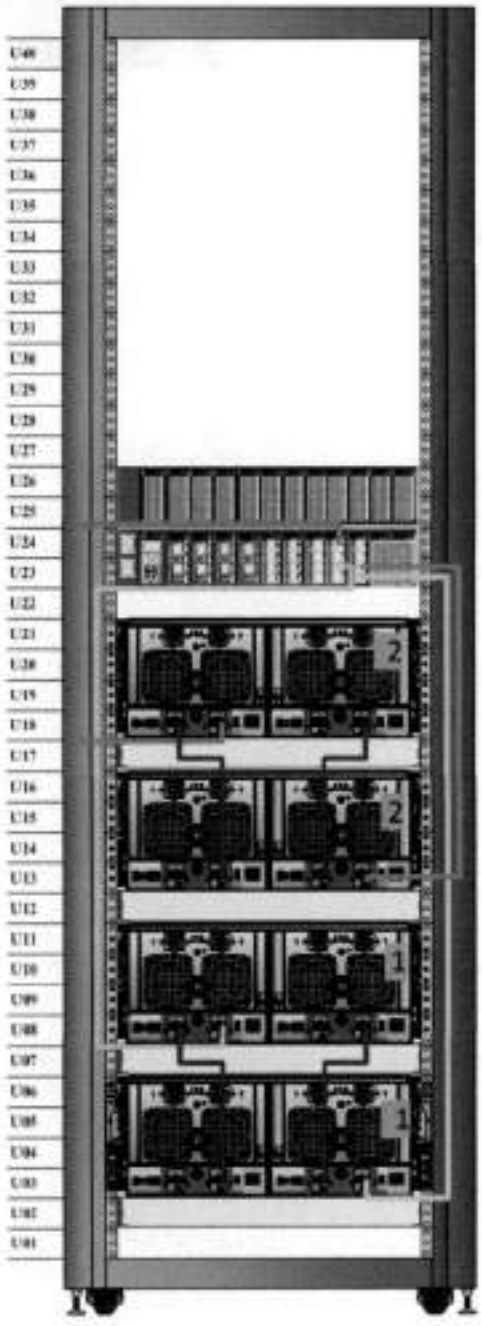


Figure 41. Recommended cabling for DD4200 (3TB drives) with Extended Retention Software

4

DD4500

This chapter contains the following topics:

Topics:

- DD4500 system features
- DD4500 system specifications
- DD4500 storage capacity
- Front Panel
- Back Panel
- I/O modules and slot assignments
- Internal system components
- DD4500 and ES30 shelf guidelines
- DD4500 and DS60 shelf guidelines

DD4500 system features

The table summarizes the DD4500 system features.

Table 23. DD4500 system features

Feature		DD4500
Rack height		4U, supported in four-post racks only
Rack mounting		Rack mount kit included with each system. Adjustable between 24 - 36 in. (60.9 - 76.2 cm).
Power		1+1 redundant, hot-swappable power units
Processor		Two 8-core processors
NVRAM		One 4-GB NVRAM module (and companion BBU) for data integrity during a power outage
Fans		Hot-swappable, redundant, 5
Memory		8 x 8 GB DIMM + 8 x 16 GB DIMM (192 GB)
Internal drives		SSD drives, 3 x 200 GB (base 10)
I/O module slots		Nine replaceable I/O module (Fibre Channel, Ethernet, and SAS) slots, one BBU, one NVRAM, and one Management module slot. See Management module and interfaces and I/O modules and slot assignments.
Supported capacity	Non-extended retention	12 x 2-TB or 8 x 3-TB shelves adding up to 285 TB of usable external capacity.
	DD Cloud Tier	285 TB of Active Tier capacity, and 570 TB of Cloud Tier capacity. 2 x 4 TB shelves are required to store DD Cloud Tier metadata.
	DD Extended Retention	32 shelves adding up to 570 TB of usable external capacity. If lower-capacity 1 TB-drive-based shelves are used, the maximum configuration will also be limited by a maximum shelf count of 40.

DD4500 system specifications

Table 24. DD4500 system specifications

Model	Watts	BTU/hr	Power	Weight	Width	Depth	Height
DD4500	800	2730	800	80 lb / 36.3 kg	17.5 in (44.5 cm)	33 in (84 cm)	7 in (17.8 cm)

Table 25. System operating environment

Operating Temperature	50° to 95° F (10° to 35° C), derate 1.1° C per 1000 feet, above 7500 feet up to 10,000 feet
Operating Humidity	20% to 80%, non-condensing
Non-operating Temperature	-40° to +149° F (-40° to +65° C)
Operating Acoustic Noise	Sound power, LWAd: 7.52 bels. Sound pressure, LpAm: 56.4 dB. (Declared noise emission per ISO 9296.)

DD4500 storage capacity

The table lists the capacities of the systems. Data Domain system internal indexes and other product components use variable amounts of storage, depending on the type of data and the sizes of files. If you send different data sets to otherwise identical systems, one system may, over time, have room for more or less actual backup data than another.

Table 26. DD4500 storage capacity

System/ Installed Memory	Internal Disks (SATA SSDs)	Data Storage Space	External Storage[1]
DD4500 (2 SAS I/O modules) 192 GB	2.5 in. 3 @ 200 GB No User Data	285 TB	Up to a maximum of 12 x 2-TB or 8 x 3-TB shelves.
DD4500 with DD Cloud Tier[1] (3 SAS I/O modules) 192 GB	2.5 in. 3 @ 200 GB No User Data	• 285 TB (Active Tier) • 96 TB (DD Cloud Tier metadata) • 570 TB (DD Cloud Tier)	Up to a maximum of 12 x 2-TB or 8 x 3-TB shelves. 2x4-TB shelves for DD Cloud Tier metadata.
DD4500 with Extended Retention software[1] (4 SAS I/O modules) 192 GB	2.5 in. 3 @ 200 GB No User Data	570 TB	Up to a maximum of 24 x 2-TB or 16 x 3-TB shelves.

[1] The capacity will differ depending on the size of the external storage shelves used. This data based on ES30 shelves.

Front Panel

The photo shows the hardware features and interfaces on the front of the system.

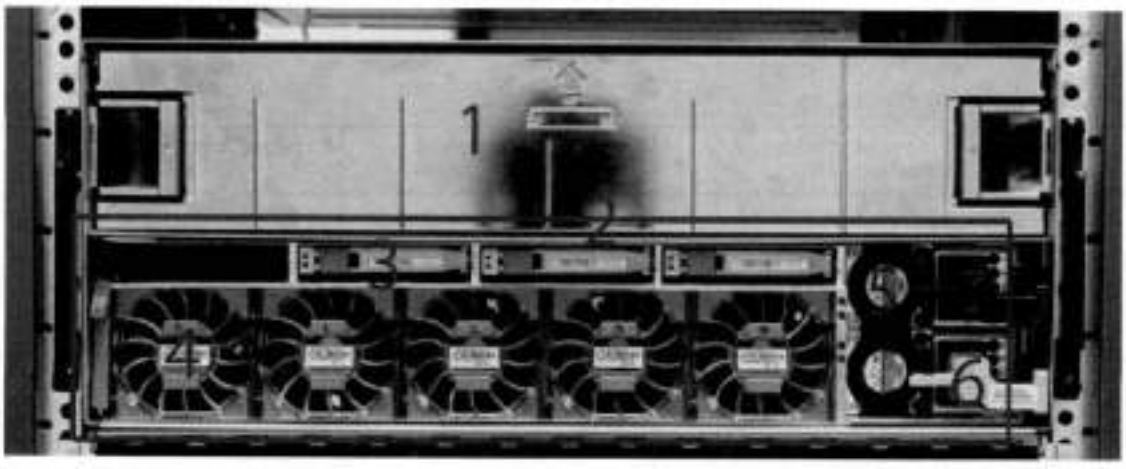


Figure 42. Front panel components

(1)	Filler panel
(2)	The red box indicates the system processor (SP) module
(3)	SSD drive #1
(4)	Fan #0
(5)	Power supply #B
(6)	AC power disconnect plug
(7)	AC power extender module

Power supply units

A system has two power supply units, numbered A and B from the bottom up. Each power supply has its own integral cooling fan. Each power unit has three LEDs (see System LED legend label) that indicates the following states:

- AC LED: Glows green when AC input is good
- DC LED: Glows green when DC output is good
- Symbol "!": Glows solid or blinking amber for fault or attention

The AC power plugs are located to the right of each power supply. These plugs are pulled to disconnect AC power to each power supply.

AC power extender module

AC power entry is connected at the rear of the system. The AC power extender module provides power to the two power supplies on the front of the system. AC Power plugs are located in the front. The module is adjacent to the SP module and can be removed and replaced.

Cooling Fans

A system contains five hot-swappable cooling fans in a 4+1 redundant configuration. The fans provide cooling for the processors, DIMMs, IO modules, and the management module. Each fan has a fault LED which causes the fan housing to glow amber. A system can run with one fan faulted or removed.

Solid-state drives

A system contains three hot-swappable 2.5" solid-state drive (SSD) bays that are located in the front and on top of the fan modules. There are four drive bays, with the left-most bay containing a blank. The next drive to the right of the blank is SSD #1, the next is #2, and the right-most bay contains SSD #3. No user backup data is kept on the SSDs.

Each drive has a blue colored power LED and an amber fault LED.

Front LED Indicators

The photo below indicates the location of the four system LEDs.

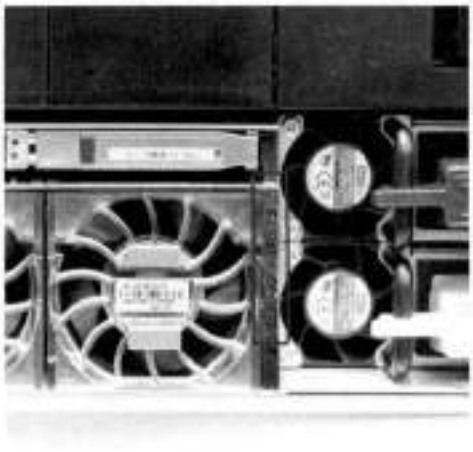


Figure 43. System LEDs

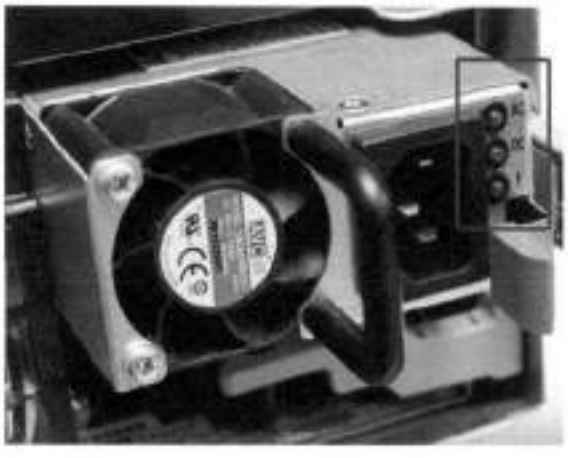
The next photo shows the location of the system LED legend label. Power supply LEDs shows the power supply LEDs. Other front LEDs are shown in Fan and SSD LEDs. LED states are described in LED status indicators.

Figure 44. System LED legend label

The power supply LEDs include:

- AC LED on top
- DC LED in the middle
- Failure LED on the bottom

Figure 45. Power supply LEDs



Each SSD has two LEDs as shown in the following figure. The lower left corner of the housing around each fan acts as an LED, glowing amber when the fan has failed.

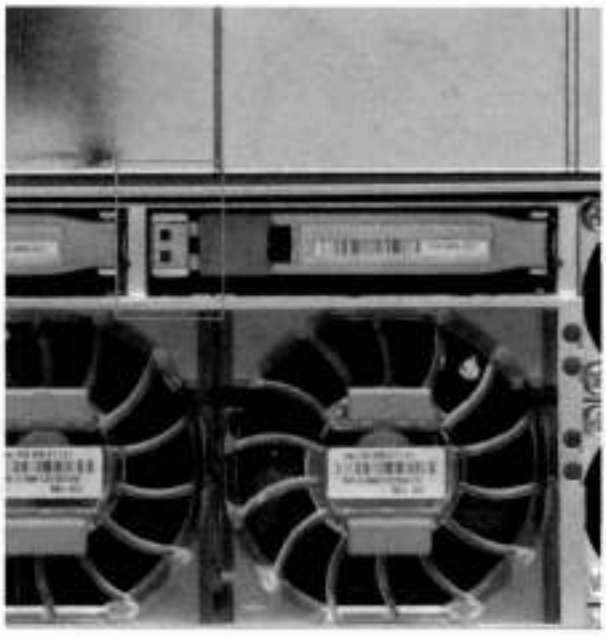


Figure 46. Fan and SSD LEDs

Table 27. LED status indicators

Part	Description or Location	State
System	Dot within a circle (top LED)	Blue indicates power on and normal operation.
System, SP fault	Exclamation point within a triangle	Dark indicates normal operation. Amber indicates failure.
System, chassis fault	Exclamation point within a triangle with a light below	Dark indicates normal operation. Yellow indicates a fault condition.
System	Marked out hand within a black square (bottom LED)	White warms not to remove the unit.
Power supply	AC LED	Steady green indicates normal AC power.
Power supply	DC LED	Steady green indicates normal DC power.
Power supply	Failure LED	Solid amber indicates a failed power supply.
SSD	Top LED	Solid blue, disk ready, blinks while busy.
SSD	Bottom LED	Dark indicates healthy. Solid amber indicates disk fail.
Fan	Fan housing	The fan housing glows an amber color during fan failure.

Back Panel

The photo shows the hardware features and interfaces on the back of the system.

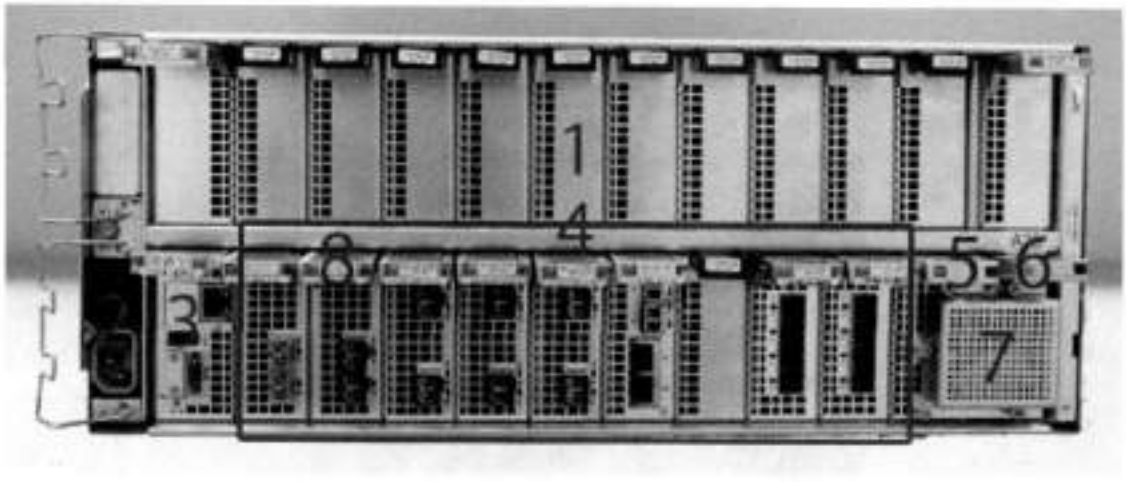


Figure 47. Features on rear of chassis

1. Upper level contains all blanks
2. AC power extender module
3. Management module (slot Mgmt A)
4. Red box indicating I/O modules (slots 0-8)
5. Battery backup (BBU in slot 9)
6. NVRAM module (slot 10)
7. Cage covering the BBU and NVRAM combination module
8. I/O LED at the end of each I/O module handle
9. Location of serial number label/tag

NOTE: For modules containing multiple ports, the bottom port is numbered as zero (0) with numbers increasing going upward.

I/O module LEDs

Each I/O module ejector handle contains a bi-colored LED. Green indicates normal function, while an amber color indicates a fault condition.

Management module and interfaces

The management module is on the left-most side when facing the back of the system, in slot Mgmt A. The process to remove and add a management module is the same as the I/O modules, however, the management module can only be accommodated in Mgmt A slot.

The management module contains one external LAN connection for management access to the SP module. One micro DB-9 connector is included to provide the console. A USB port is provided for use during service of the system to allow booting from a USB flash device.

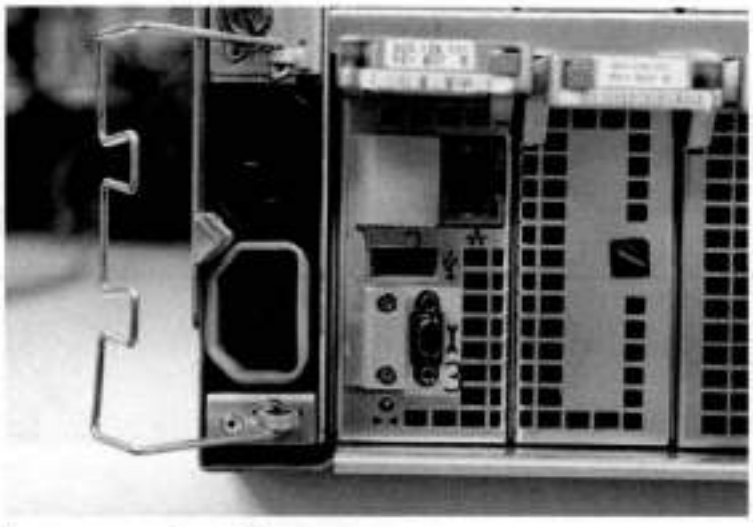


Figure 48. Interfaces on the management module

- 1 - Ethernet port
- 2 - USB port
- 3 - Micro serial port

I/O modules and slot assignments

The table shows the I/O module slot assignments for the systems. See Features on rear of chassis for a view of the slot positions on the back panel and Top view of SP module with SP cover removed for a top view.

Table 28. DD4500 slot assignments

Slot Number	DD4500	DD4500 with Extended Retention Software	DD4500 with DD Cloud Tier
MGMT A	Management module	Management module	Management module
0	Fibre Channel (FC), Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
1	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
2	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
3	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
4	Ethernet or empty	Ethernet or empty	Ethernet or empty
5	Ethernet or empty	SAS	Ethernet or empty
6	Empty	SAS	SAS
7	SAS	SAS	SAS
8	SAS	SAS	SAS
9	BBU	BBU	BBU
10	NVRAM	NVRAM	NVRAM

Slot addition rules

- A maximum of six optional I/O modules (FC plus Ethernet) are allowed in systems without Extended Retention software, and a maximum of five optional I/O modules (FC plus Ethernet) are allowed in systems with Extended Retention software.
- Additional FC modules should be installed in numerically increasing slot numbers immediately to the right of the existing FC modules, or starting in slot 0 if no FC modules were originally installed. A maximum of four FC modules are allowed in a system.
- Additional Ethernet modules should be installed in numerically decreasing slot numbers immediately to the left of the existing Ethernet modules or starting in slot 4 if no Ethernet modules were originally installed. For systems without Extended Retention software, a maximum of six (limited to four of any one type) Ethernet modules can be present. For systems with Extended Retention software, a maximum of five (limited to four of any one type) Ethernet modules can be present.
- All systems include two SAS modules in slots 7 and 8. Systems with Extended Retention software must have two additional SAS modules in slots 5 and 6.
- For systems without Extended Retention software, if adding I/O modules results in the allowed maximum of six I/O modules present, slot 5 is used. Slot 5 is only used for an Ethernet module. Adding FC modules in this specific case require moving an existing Ethernet module to slot 5. Other than this specific case, it is not recommended to move I/O modules between slots.
- Adding Extended Retention software to a system includes adding two SAS modules in slots 5 and 6. If the system originally had the maximum of 6 optional I/O modules, the I/O module in slot 5 must be permanently removed from the system.

Fibre Channel (FC) I/O Module Option

An FC I/O module is a dual-port Fibre Channel module. The optional virtual tape library (VTL) feature requires at least one FC I/O module. Boost over Fiber Channel is optional and the total FC HBAs cannot exceed more than allowable Fibre Channel cards per controller.

Ethernet I/O Module Options

The available Ethernet I/O modules are:

- Dual Port 10GBase-SR Optical with LC connectors

- Dual Port 10GBase-CX1 Direct Attach Copper with SPF+ module
- Quad Port 1000Base-T Copper with RJ-45 connectors
- Quad port 2 port 1000Base-T Copper (RJ45) /2 port 1000Base-SR Optical

Internal system components

The photo shows the system with the system processor (SP) module that is removed from the chassis and the SP cover removed.

Figure 49. Top view of SP module with SP cover removed

- 1 - Front of system
- 2 - Four groups of 4 DIMM cards

DIMM modules

DD4500 systems contain 8 x 8 GB and 8 x 16 GB of memory DIMM. DIMMs must be in specific slots based on DIMM size.

DD4500 and ES30 shelf guidelines

The Data Domain system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your Data Domain system as listed in the following table below.
- Use the Installation and Setup Guide for your Data Domain system to minimize the chance of a cabling mistake.
- A Data Domain system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.
- ES30 SATA shelves must be on their own chain.

NOTE:

- ES30 SAS shelves must be running DD OS 5.4 or later.
- ES30-45 SATA shelves must be running DD OS 5.4 or later.
- DD OS 5.7 and later support 4TB drives.

Table 29. DD4500 and ES30 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	ES30 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB) [1]	Max RAW external capacity (TB) [2]
DD4500	192	2x4	SAS 30, 45, 60; SATA 15, 30, 45[5]	5[6]	4	288	384
DD4500 ER [3, 4]	192	4x4	SAS 30, 45, 60; SATA 15, 30, 45[5]	7	8	576	768
DD4500 w/ DD Cloud Tier	192	3x4	SAS 30, 45, 60; SATA 15, 30, 45[5]	7	8	288 (max), additional 96 SAS dedicated to DD Cloud Tier	384 (max), additional 120 SAS dedicated to DD Cloud Tier

1. This figure only counts drives that have user data in the shelves.

2. The raw capacity of an ES30 is 125% of the available capacity.

3. The maximum shelf count for any specific drive/shelf size might be less than the product of max shelves x max shelves per set.

4. With Extended Retention software.

5. ES30-45 (SATA) is only supported with DD OS 5.4 or later.

6. 5 shelves maximum with ES30, 4 is the recommended maximum.

Single phase power connections for 40U-P (current racks)

The following figures show single phase power connections for several Data Domain systems.

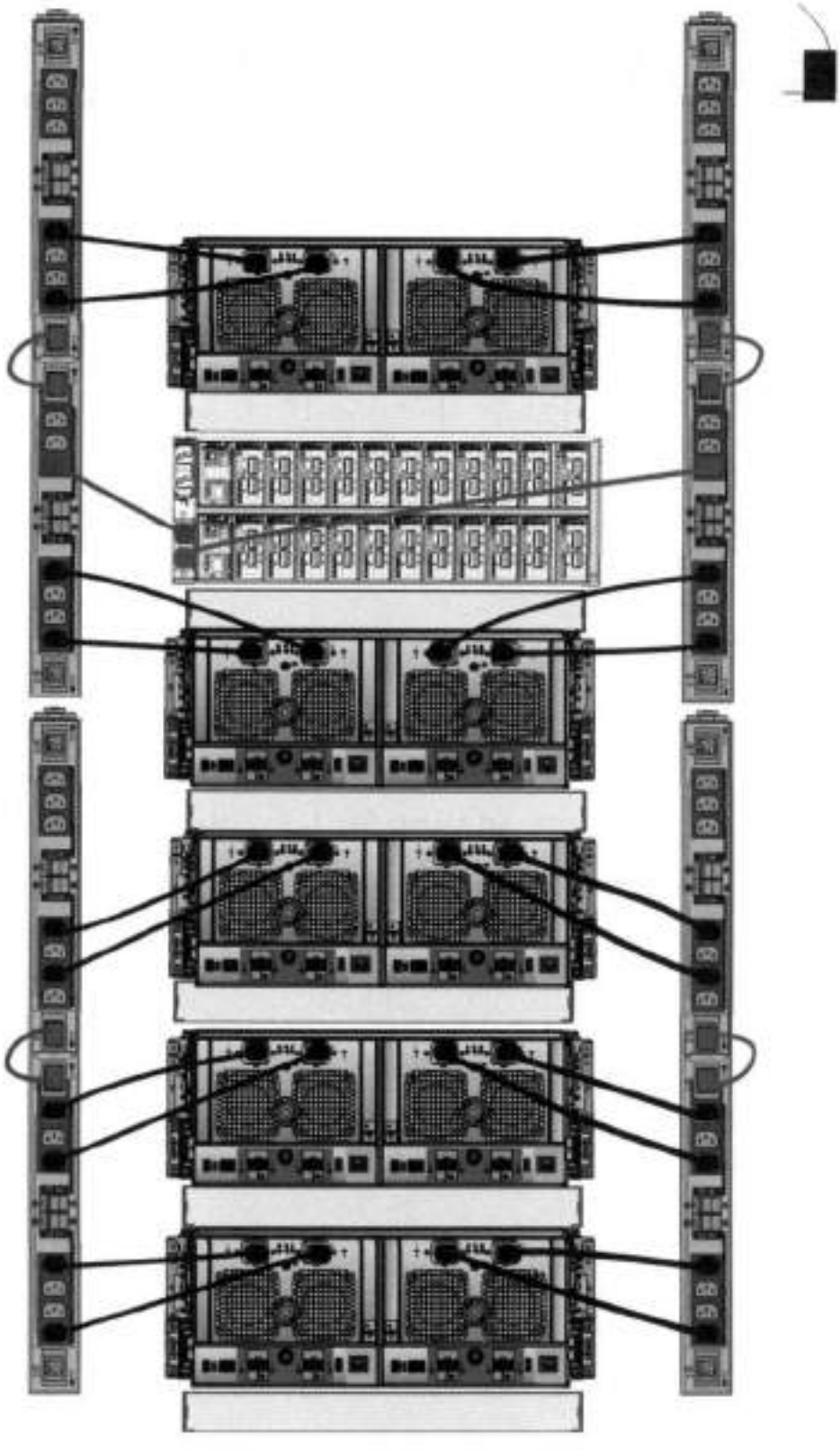


Figure 50. Single phase power connections for DD4200, DD4500, and DD7200 systems

Cabling shelves

NOTE:

- Before cabling the shelves, physically install all shelves in the racks. Refer to the rail kit installation instructions included with the ES30 shelf for rack mounting.
- The documentation refers to two SAS HBAs. If only one HBA is allowed in a system, then use another port as defined later for that specific system.
- On an HA system, add cables from the second node to open ports at the end of the sets. The ports on the second node must connect to the same sets as the corresponding ports on the first node.

Ports on the system's SAS HBA cards connect directly to a shelf controller's host port. For redundancy, you need to create dual paths by using a port on one SAS HBA card to connect to one shelf controller in each shelf set, and a port on another SAS HBA card to connect to another shelf controller in the same shelf set. With dual paths, if one SAS HBA card fails, the shelf is still operational. However, in the unlikely event any single shelf becomes completely disconnected from power or SAS cables and becomes disconnected from a previously operational shelf, the file system goes down and the shelf is not operational. This is considered a double failure.

There are two kinds of configurations: one shelf in a set or multiple shelves in a set.

ES30 and DD4500 cabling

There are a few rules that must be followed when adding a mixture of ES20, ES30 SATA, and ES30 SAS shelves to your system. If a system does not follow ALL of these rules it is not a legitimate configuration.

Prerequisites:

- Follow the minimum and maximum shelf capacity configuration provided in the table.
- You cannot have ES20 and ES30 shelves in the same set.
- You cannot have ES30 SATA and ES30 SAS shelves in the same set.
- You cannot exceed the maximum amount of raw capacity displayed in the product's cabling table.
- The maximum number of shelves displayed in the product's cabling table cannot be exceeded.
- You cannot have more than four ES20s in a single set (maximum preference is three).
- You cannot have more than five ES30s in a single set (maximum preference is four).
- You can have a maximum of seven ES30s for systems with Extended Retention software.
- There are no specific placement or cabling requirements for the metadata shelves for DD Cloud Tier configurations. These shelves can be installed and cabled the same way as standard ES30 shelves.

NOTE: An ES20 requires more power than an ES30. Ensure that your rack is configured to handle the power needs.

The tables below show how to configure a mixed system. To use the tables, go to the appropriate system. Then find the number of ES20s that are to be configured in the first column. The next column defines the number of ES20 sets. If there are multiple rows with the same number of ES20s then pick the row with the appropriate number of ES20 SATA shelves. The next column in that row defines the number of sets of ES30 SATA shelves. Finally, there may be entries for the number of desired ES30 SAS shelves and the number of sets to be used.

If the combinations of shelves exceed the supported usable storage, there may not be an entry. The entries are based on the smallest usable storage per shelf type (12TB for ES20, 12 TB for ES30 SATA, and 24TB for ES30 SAS). Always check that the sum of the usable storage of all of the shelves does not exceed the supported usable storage of the configuration.

Table 30. Minimum and maximum configurations

System	Minimum appliance shelf count	Maximum appliance shelf count	DD Cloud Tier systems in TB	Extended Retention systems (ER) in TB	Max shelves for ER
4500 (288)	2	20	• 285 • 120 for metadata	• DD OS 5.4 and earlier: 1152 • DD OS 5.5 and later: 576	40

Systems without Extended Retention or DD Cloud Tier all support four chains. The following tables show combinations of ES20 and ES30 shelves. For combinations of any two types of shelves, these tables can be used as a guide.

Table 31. DD4500 cabling information

DD4500					
ES20	ES20 chains	ES30 SATA	ES30 SATA chains	ES30 SAS	ES30 SAS chains

Table 31. DD4500 cabling information (continued)

DD4500					
13-16	4	0	0	0	0
9-12	3	1-5	1	0	0
9-12	3	0	0	1-5	1
5-8	2	1-5	1	1-5	1
5-8	2	6-8	2	0	0
5-8	2	0	0	1-5	1
5-8	2	0	0	6-10	2
1-4	1	9-12	3	0	0
1-4	1	5-8	2	1-5	1
1-4	1	1-4	1	1-5	1
1-4	1	1-4	1	6-10	2
1-4	1	0	0	1-4	1
1-4	1	0	0	5-8	2
1-4	1	0	0	9-11	3
0	0	16-21	4	0	0
0	0	11-15	3	1-5	1
0	0	6-10	2	1-4	1
0	0	6-10	2	5-9	2
0	0	1-5	1	1-4	1
0	0	1-5	1	5-8	2
0	0	1-5	1	9-11	3
0	0	0	0	1-4	1
0	0	0	0	5-8	2
0	0	0	0	9-12	3

The following figures show cabling for base systems, systems with the Extended Retention software option, and systems integrated with an Avamar system.

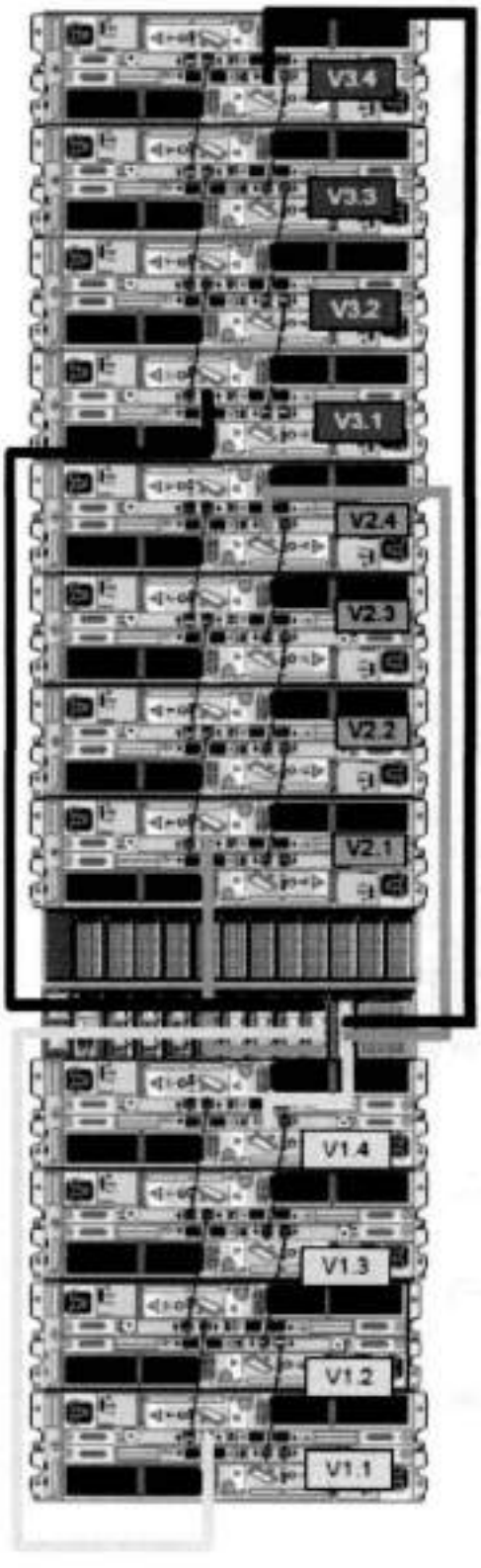


Figure 51. Recommended DD4500 cabling

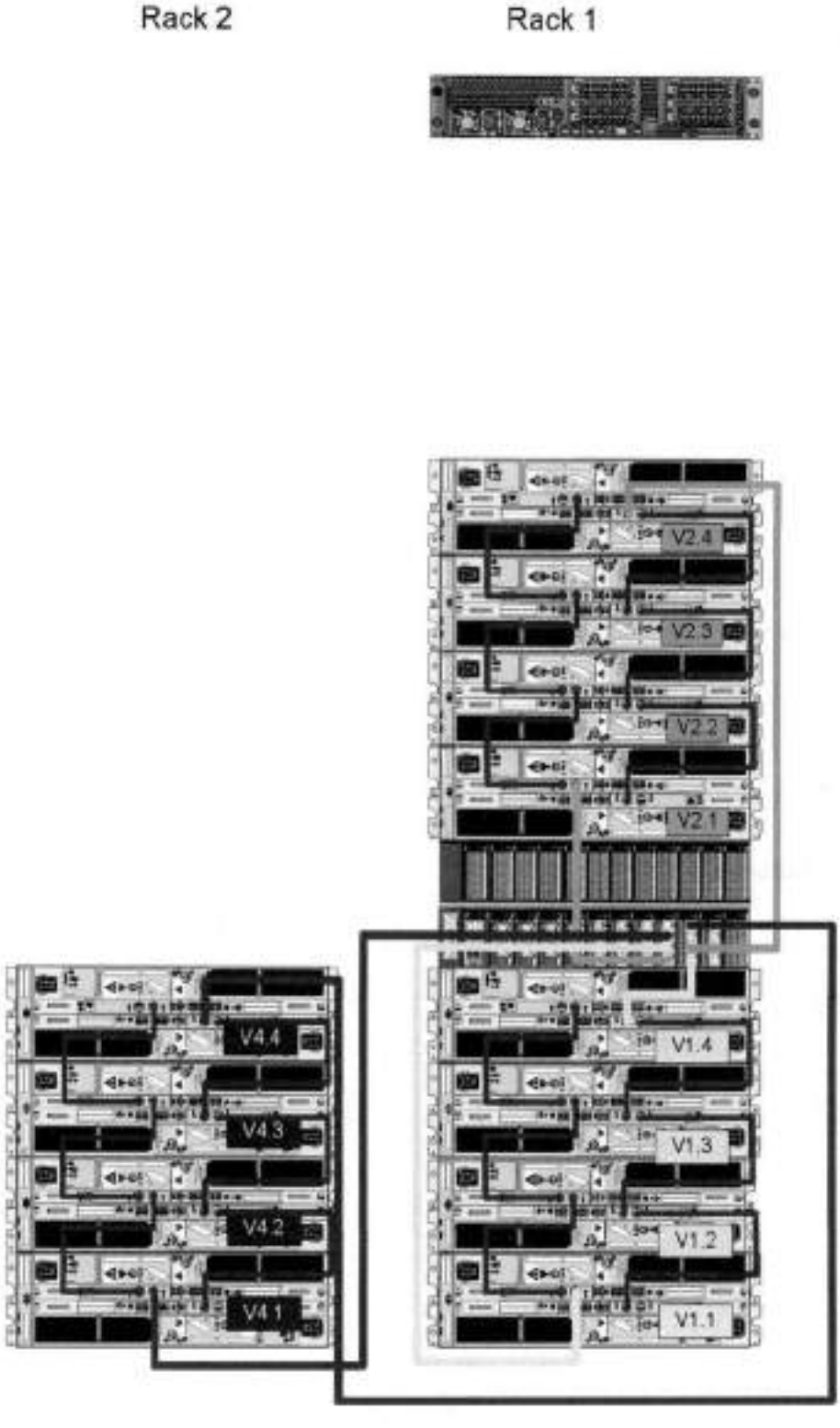


Figure 52. Recommended cabling for DD4500 integrated with Avamar

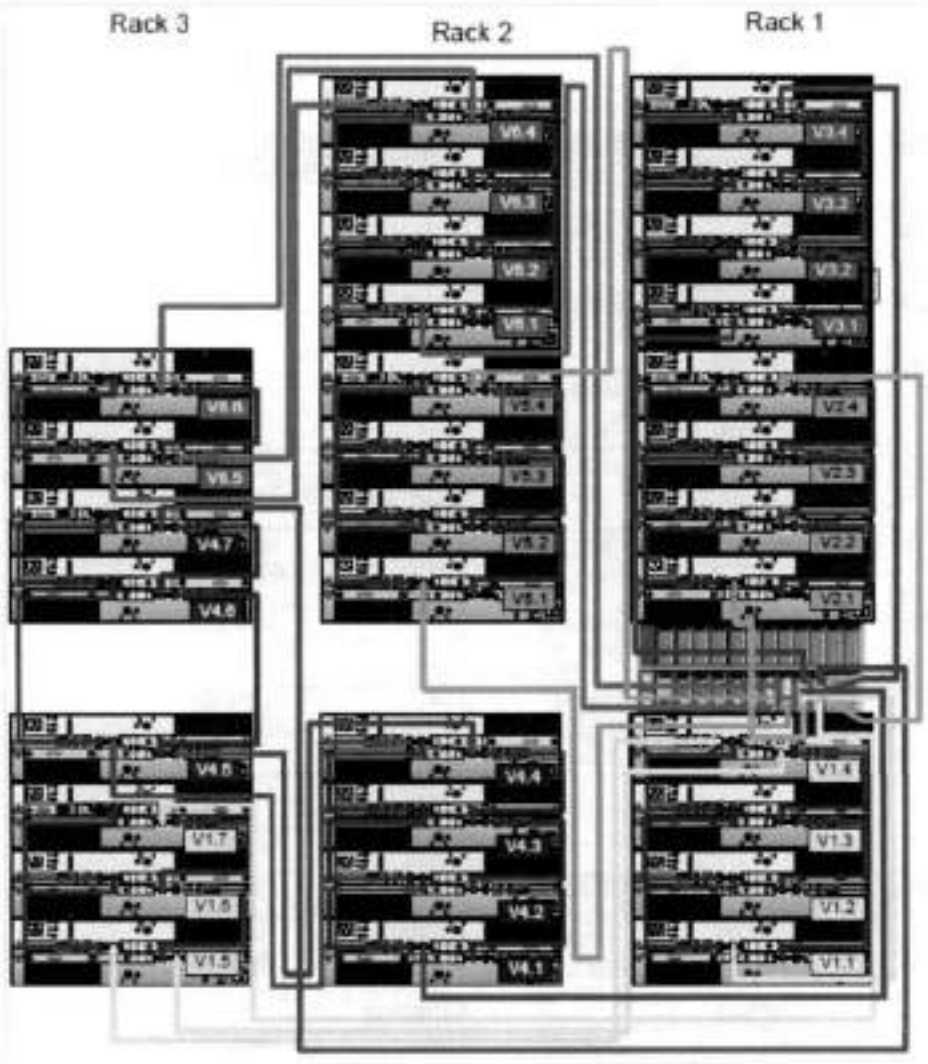


Figure 53. Recommended cabling for DD4500 with extended retention software or DD Cloud Tier

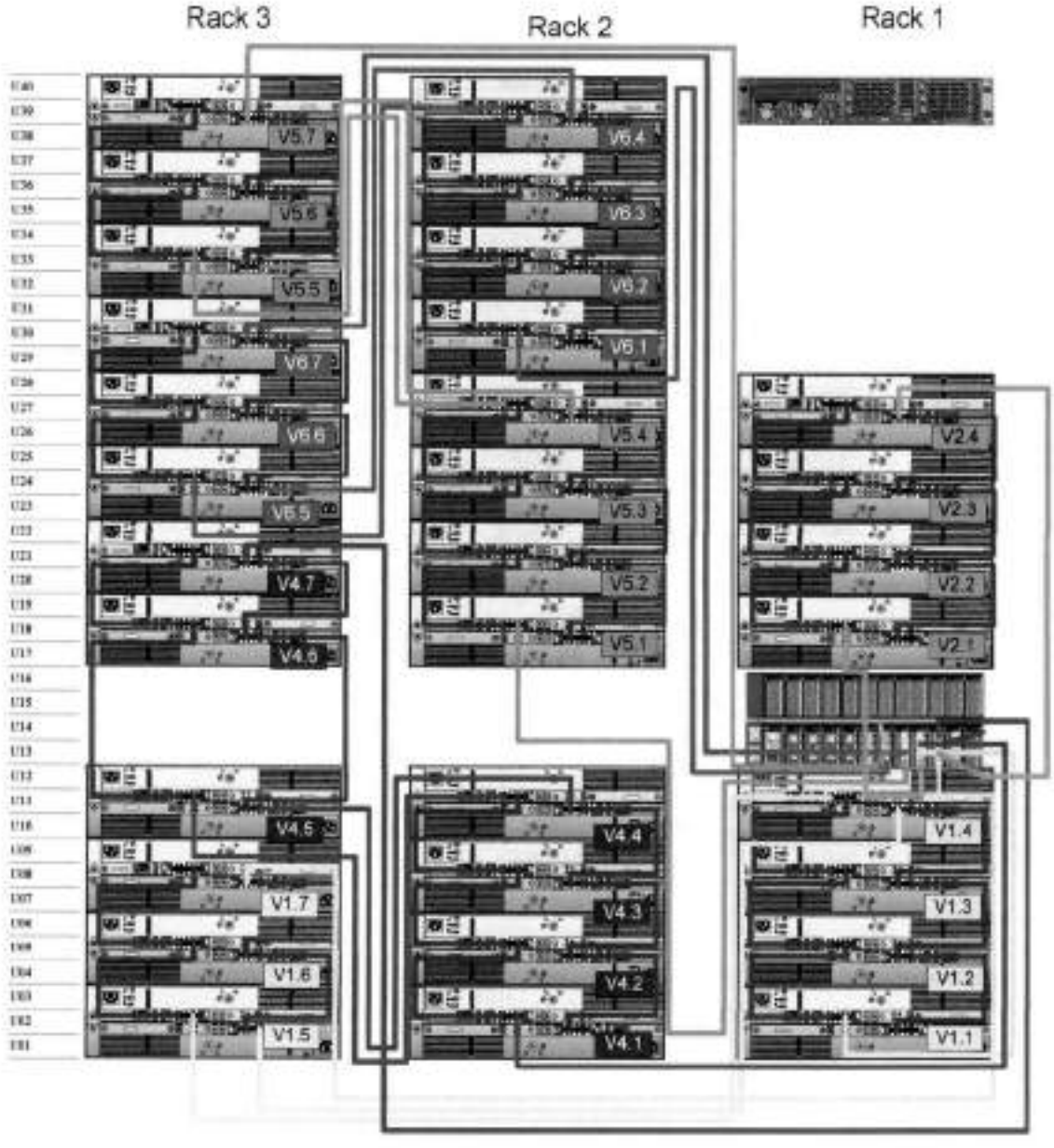


Figure 54. Recommended cabling for DD4500 with extended retention and integrated with Avamar

DD4500 and DS60 shelf guidelines

The Data Domain system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your Data Domain system as listed in the following table.
- For redundancy, the two connections from a Data Domain system to a set of shelves must use ports on different SAS I/O modules.
- Use the Installation and Setup Guide for your Data Domain system to minimize the chance of a cabling mistake.
- A Data Domain system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.
- ES30 SATA shelves must be on their own chain.

- If ES30 SAS shelves are on the same chain as a DS60, the maximum number of shelves on that chain is 5.
- DD OS 5.7.1 does not support HA with SATA drives.

Table 32. DD4200 and DS60 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	DS60 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB)[1]	Max RAW external capacity (TB)
DD4500	192	2x4	SAS 45, 60	2	4	288	360
DD4500 ER [2]	192	4x4	SAS 45, 60	2	8	576	720

NOTE: An entry of 45 corresponds to DS60-3 models and an entry of 60 corresponds to DS60-4 models.

1. This column only counts drives that have user data in the shelves. For example, a DS60 4-240 has 192TB.

2. With Extended Retention software.

Single phase power connections for 40U-P (current racks)

The following figures show single phase power connections for several Data Domain systems.

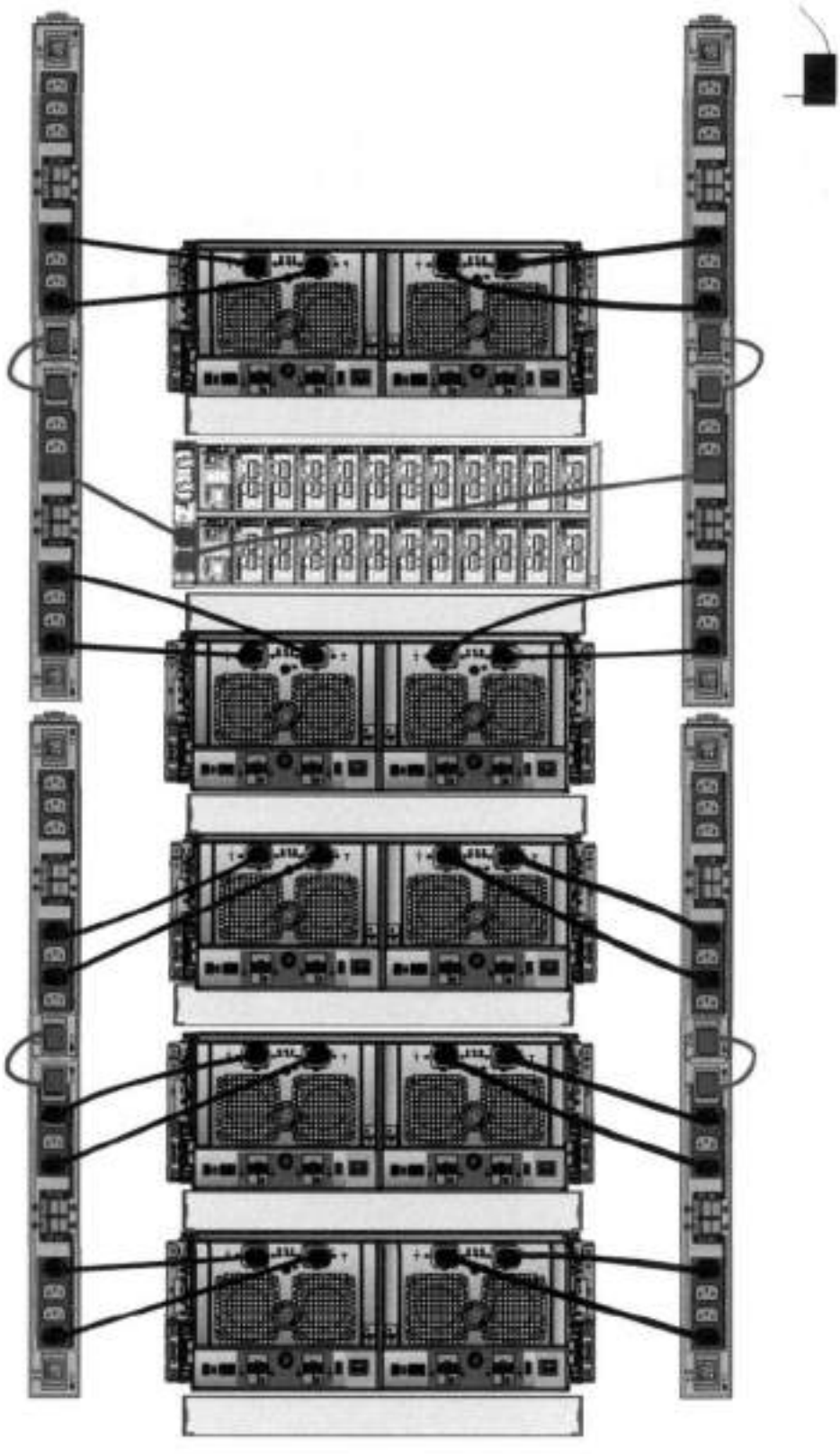


Figure 55. Single phase power connections for DD4200, DD4500, and DD7200 systems

3-phase power connections for 40U-P (current racks)

Some environments use 3-phase power for 40U-P racks used for several Data Domain systems. In those situations it is desirable to balance the current draw across all 3 phases. The recommended 3-phase power cabling attempts to do that, but an optimal

configuration is dependent on the specific installation. The following figures show recommended 3-phase power connections for several Data Domain systems.

NOTE: The next few diagrams show recommended 3-phase delta power connections.

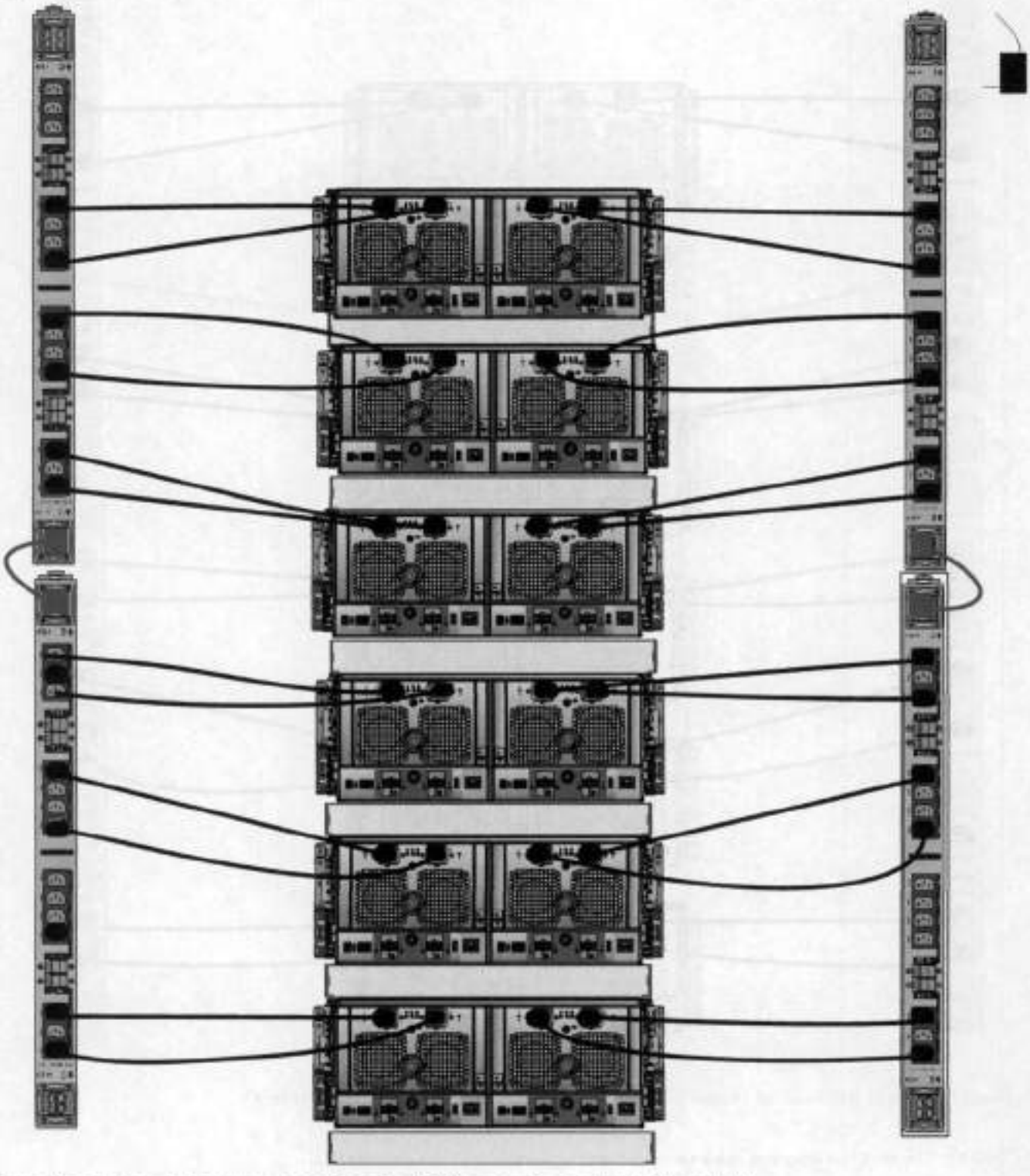


Figure 56. 3-phase delta power connections for DS60 expansion shelves (full-racked)

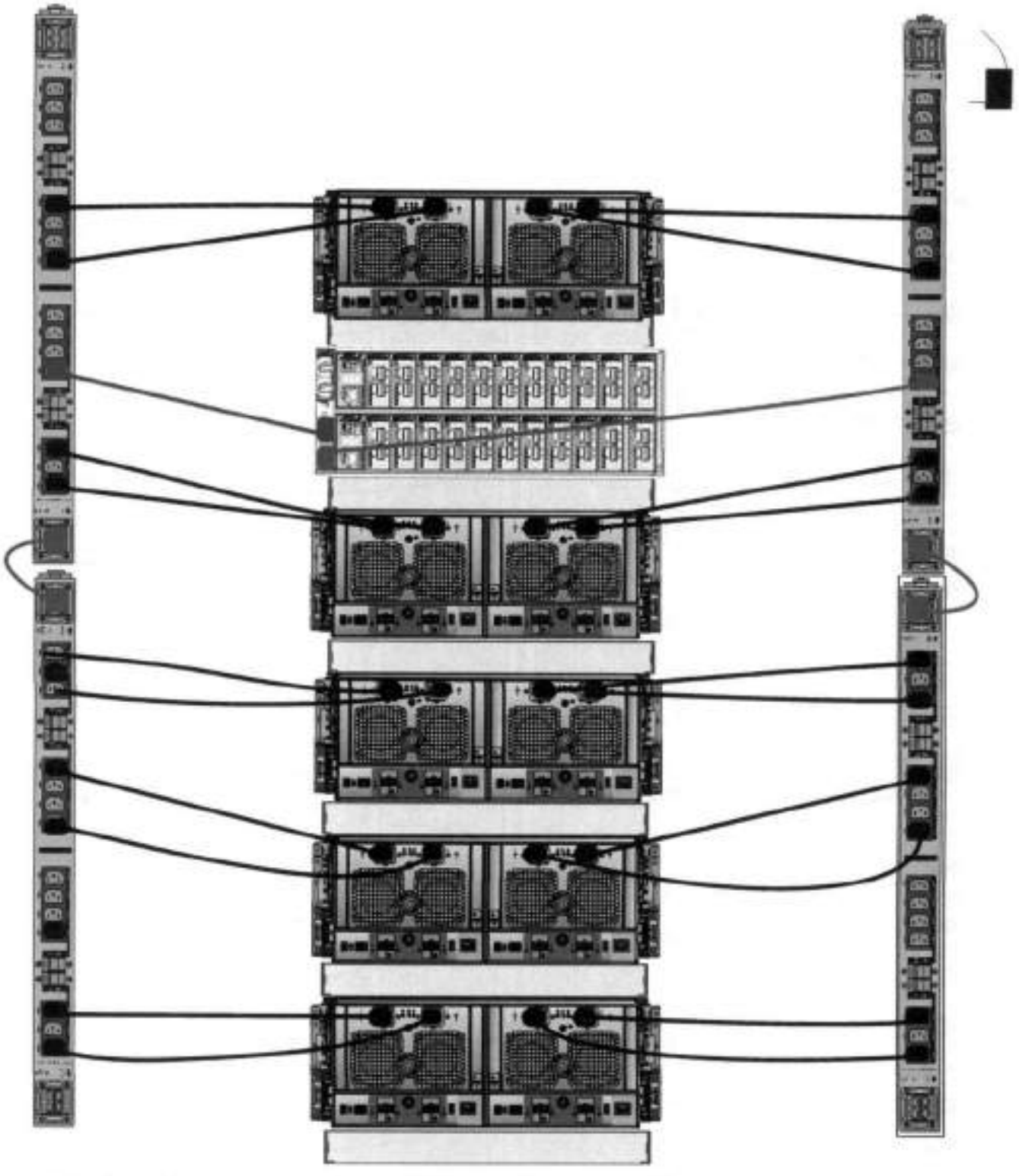


Figure 57. 3-phase delta power connections for DD4200, DD4500, and DD7200 systems

NOTE: The next few diagrams show recommended 3-phase wye power connections.

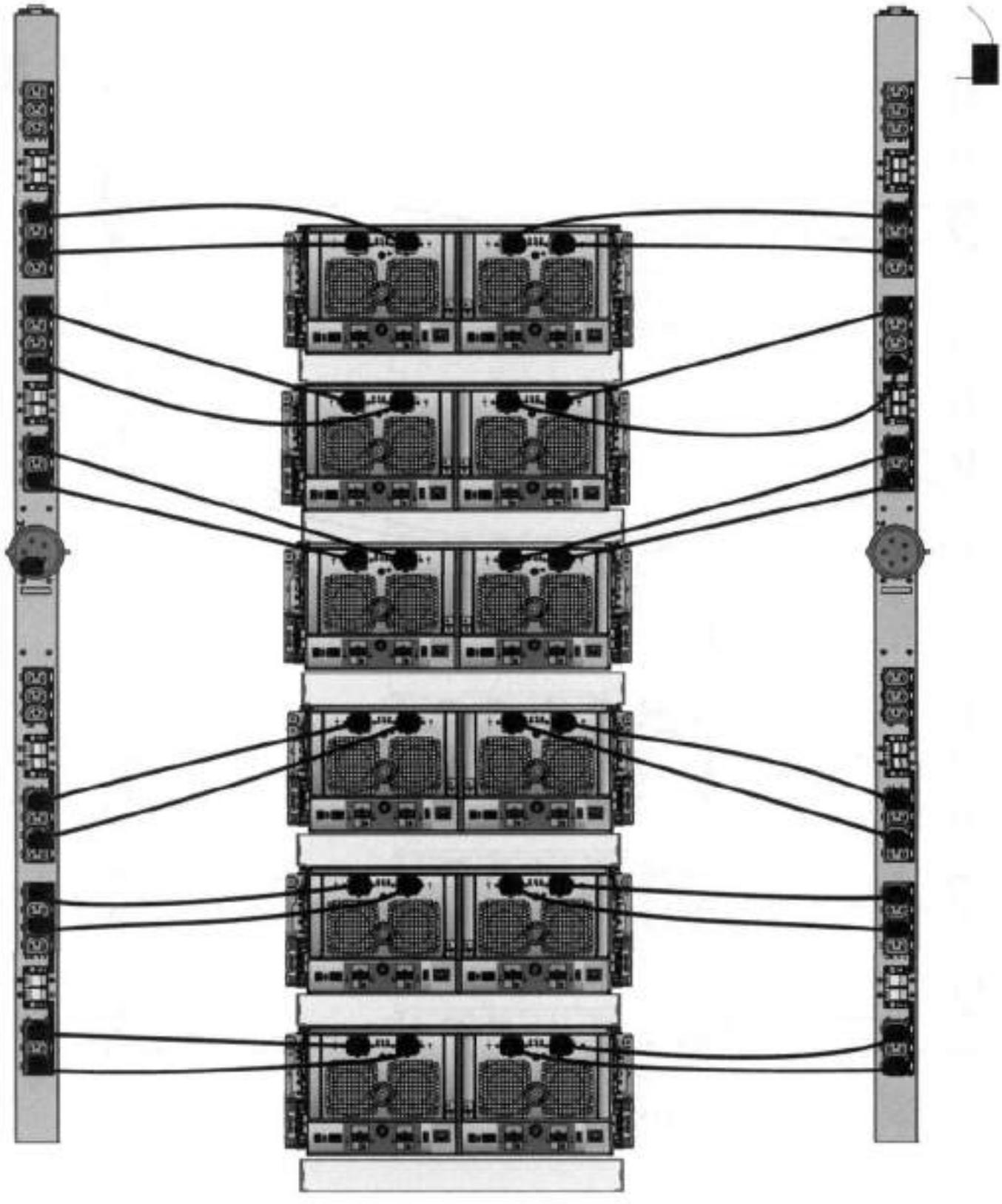


Figure 58. 3-phase wye power connections for DS60 expansion shelves (full-racked)

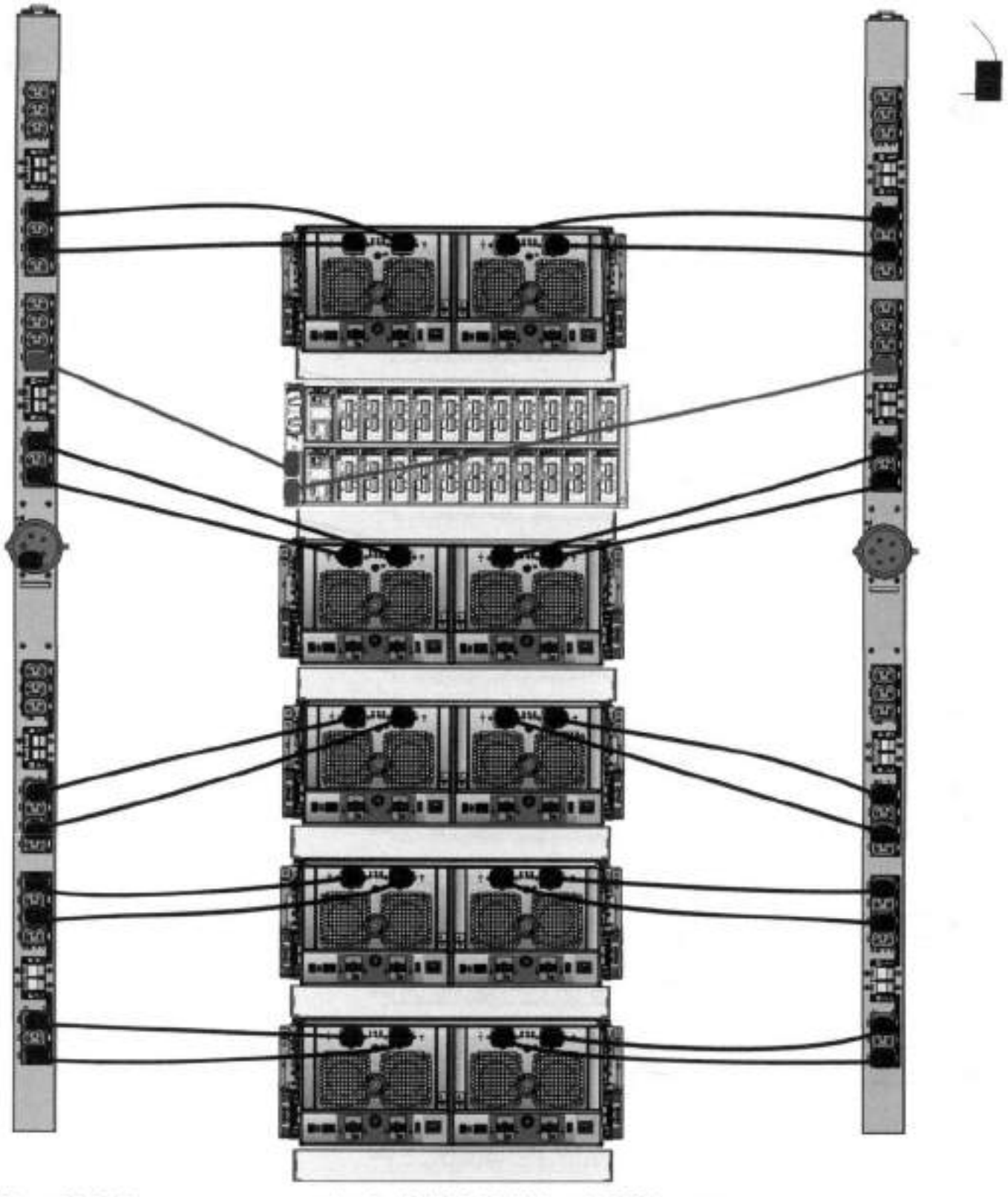


Figure 59. 3-phase wye power connections for DD4200, DD4500, and DD7200 systems

DS60 and DD4500 cabling

There are a few rules that must be followed when adding a mixture of DS60 and other shelf types to your system.

CAUTION: **If a system does not follow all these rules, it is not a legitimate configuration.**

Prerequisites:

- You cannot exceed the maximum amount of usable capacity displayed in cabling table for each system.
- You cannot exceed the maximum number of shelves displayed in cabling table for each system.
- You cannot connect more than two DS60 shelves in a single set.

Table 33. Minimum and maximum configurations

System	Appliance maximum	Minimum appliance shelf count
DD4500	288 TB	1

Mixing DS60, ES30, and ES20 shelves:

The non-Extended Retention versions of these systems all support four chains.

Extra planning and reconfiguration may be required to add DS60 shelves to system with ES20 shelves, ES30 SATA shelves, or a combination of shelves.

- The ES20 shelves must be on their own set. Minimize the ES20 set count by combining up to four ES20s per set.
- ES30 SATA shelves must also be on their own sets. Minimize the ES30 set count by combining up to five ES30s per set. If required, combine up to seven ES30 SAS shelves per set to minimize the set count.
- A set can contain a maximum of two DS60 shelves and, if required because of other restrictions, add ES30 SAS shelves up to a maximum of five shelves in that set.

NOTE: The configuration rules apply also to Extended Retention systems.

The following figures show cabling for base systems and systems with the Extended Retention software.

NOTE: It is recommended that the DS60 shelf with the greater number of drives should always be placed in the bottom position.

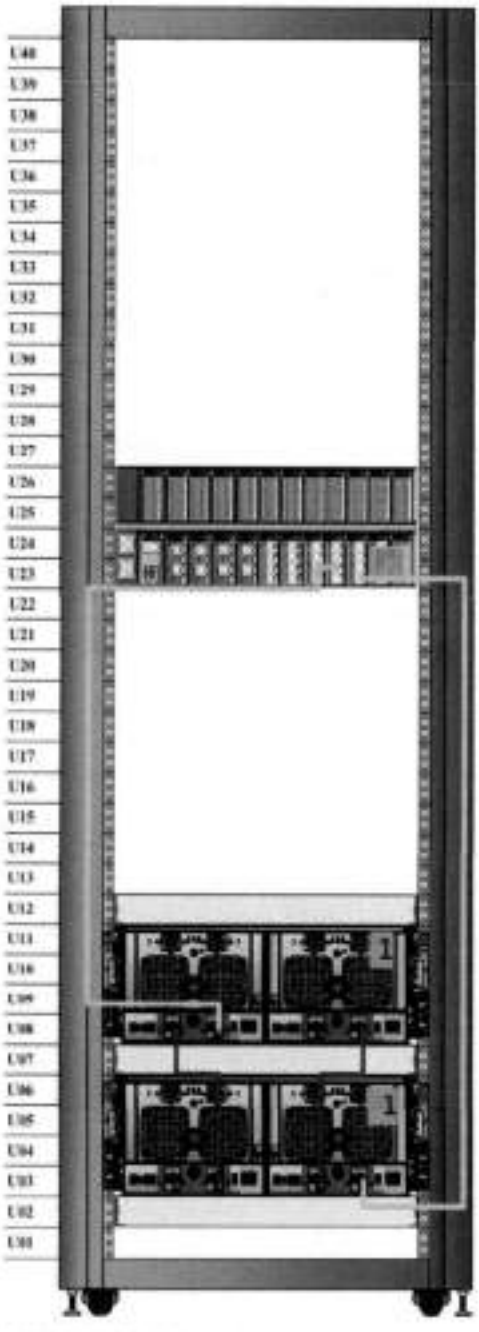


Figure 60. Recommended cabling for DD4500 (3TB drives)

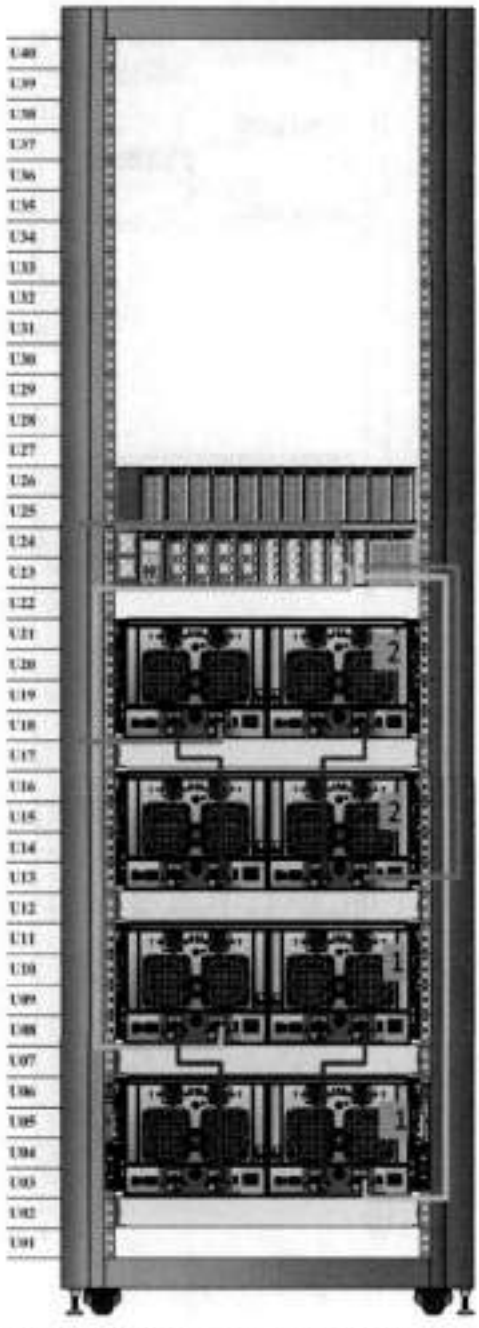


Figure 61. Recommended cabling for DD4500 (3TB drives) with Extended Retention software

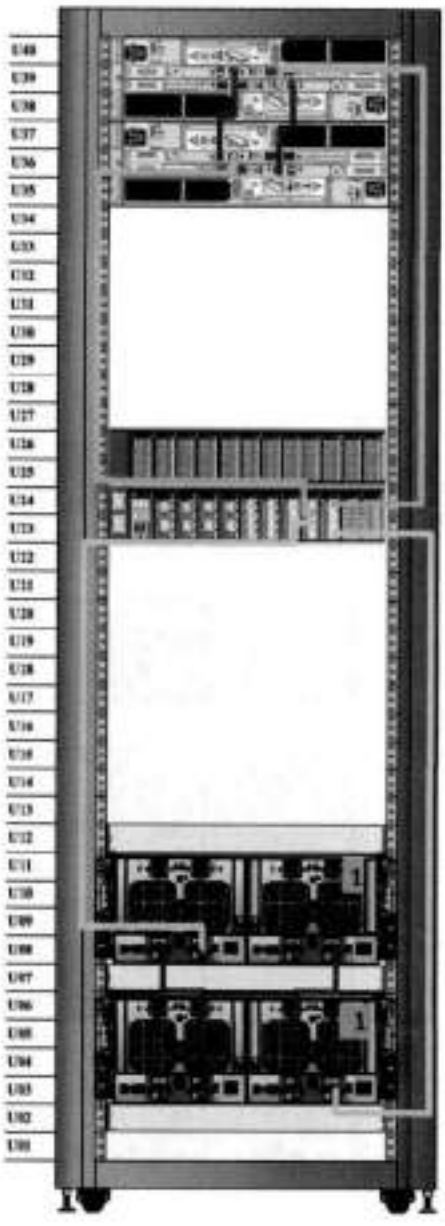


Figure 62. Recommended cabling for DD4500 with DD Cloud Tier

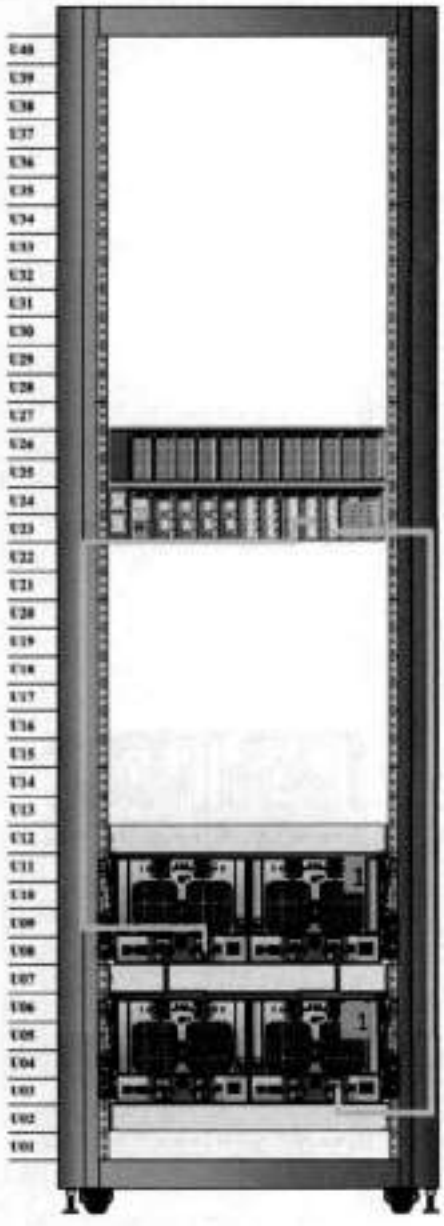


Figure 63. Recommended cabling for DD4500 (4TB drives)

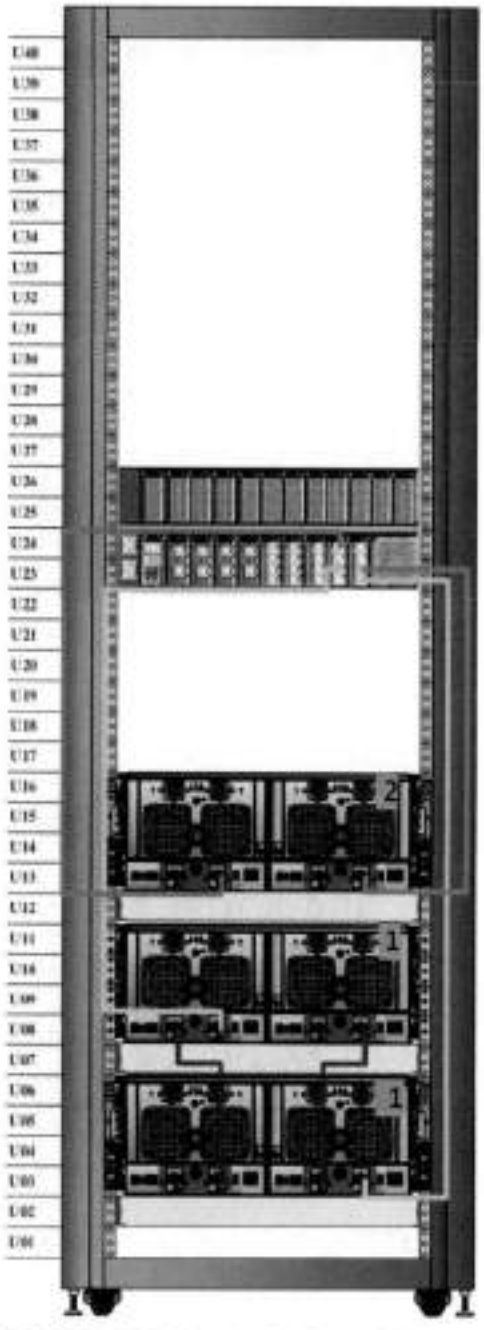


Figure 64. Recommended cabling for DD4500 (4TB drives) with Extended Retention software

5

DD6300

This chapter contains the following topics:

Topics:

- DD6300 system features
- DD6300 system specifications
- DD6300 storage capacity
- DD6300 front panel
- Back panel
- I/O modules
- Internal system components
- DD6300 and ES30 shelf guidelines
- DD6300 and DS60 shelf guidelines

DD6300 system features

Table 34. DD6300 system features

Feature		Base configuration	Expanded configuration
Rack height		2U	2U
Processor		E5-2620 V3	E5-2620 V3
Kernel		3.2.x	3.2.x
NVRAM		NVRAM 8g Model 3	NVRAM 8g Model 3
Memory		6 x 8 GB DIMM (48 GB)	12 x 8 GB DIMM (96 GB)
Internal drives	HDDs in 3.5" bays	7/ 7+5	12
	SSDs in 3.5" bays	0	0
	SSDs in 2.5" bays	1	2
I/O module slots	SAS I/O modules (Quad Port 6 Gbps SAS)	• 0 for internal storage only • 1 with external storage	• 0 for internal storage only • 1 with external storage
	Network and FC I/O modules	Four replaceable I/O module slots. Not hot-swappable.	Four replaceable I/O module slots. Not hot-swappable.
Supported capacity		76 TB (28 TB internal + 48 TB external)	180 TB (36 TB internal + 144 TB external)
High availability support		No	No
HA private interconnect		N/A	N/A
External SSD shelf		N/A	N/A
SAS string depth (max)	ES30	1	4
	DS60	0	1
Stream count		270 writes, 75 reads	270 writes, 75 reads

DD6300 system specifications

Table 35. DD6300 system specifications

Average power consumption 25 C	Heat dissipation (operating maximum)	Weight [a]	Width	Depth	Height
530W	1.69 x 10^6 J/hr (1604 Btu/hr) maximum	80 lbs (36.29 kg)	17.50 in (44.45 cm)	30.5 in (77.5 cm)	3.40 in (8.64 cm)

a. The weight does not include mounting rails. Allow 2.3-4.5 kg (5-10 lb) for a rail set.

Table 36. System operating environment

Requirement	Description
Ambient temperature	10°C - 35°C; derate 1.1°C per 1,000 ft (304 m)
Relative humidity (extremes)	20–80% noncondensing
Elevation	0 - 7,500ft (0 - 2,268m)
Operating acoustic noise	L_{wad} sound power, 7.5 Bels

DD6300 storage capacity

The following table provides storage capacity information for the DD6300 system.

Table 37. DD6300 storage capacity

Memory	Internal disks	Internal storage (raw)	External storage (raw)	Usable data storage space (TB/TiB/GB/GiB)[a]			
48 GB (Factory base)	• Front: 7 x 4 TB • Rear: 1 x 800 GB SSD	28 TB	60 TB	• Internal: 14 TB • External: 48 TB	• Internal: 12.74 TiB • External: 43.68 TiB	• Internal: 14,000 GB • External: 48,000 GB	• Internal: 13,039 GiB • External: 44,704 GiB
48 GB (Factory upgrade)	• 12 x 4 TB HDD • Rear: 1 x 800 GB SSD	48 TB	60 TB	• Internal: 34 TB • External: 48 TB	• Internal: 30.94 TiB • External: 43.68 TiB	• Internal: 34,000 GB • External: 48,000 GB	• Internal: 31,665 GiB • External: 44,704 GiB
48 GB (Field Upgrade)	• (7 + 5) x 4 TB HDD • Rear: 1 x 800 GB SSD	48 TB	60 TB	• Internal: 22 TB • External: 48 TB	• Internal: 20.02 TiB • External: 43.68 TiB	• Internal: 22,000 GB • External: 48,000 GB	• Internal: 20,489 GiB • External: 44,704 GiB
96 GB (Expanded)	• Front: 12 x 4 TB HDDs • Rear: 2 x 800 GB SSD	48 TB	180 TB	• Internal: 34 TB • External: 144 TB	• Internal: 30.94 TiB • External: 131 TiB	• Internal: 34,000 GB • External: 144,000 GB	• Internal: 31,665 GiB • External: 134,110 GiB
96 GB (Field upgrade	• Front: (7 + 5) x 4 TB HDDs	48 TB	180 TB	• Internal: 22 TB • External: 144 TB	• Internal: 20.02 TiB • External: 131 TiB	• Internal: 22,000 GB • External: 144,000 GB	• Internal: 20,489 GiB • External: 134,110 GiB

Table 37. DD6300 storage capacity (continued)

Memory	Internal disks	Internal storage (raw)	External storage (raw)	Usable data storage space (TB/TiB/GB/GiB)[a]			
from 48 GB)	• Rear: 2 x 800 GB SSD						

a. The capacity differs depending on the size of the external storage shelves used. This data based on ES30 shelves.

DD6300 front panel

DD6300 All-in-One (AIO) systems have one of the following front panel drive configurations to host the DD OS boot drives, and provide storage for customer data:

NOTE: Upgrading a base configuration to an expanded configuration provides less capacity than a factory-built expanded configuration.

Table 38. DD6300 AIO capacity

Configuration	Installed drives	Usable internal capacity
DD6300 base configuration	Seven 4 TB HDDs	14 TB
DD6300 expanded configuration (factory)	Twelve 4 TB HDDs	34 TB
DD6300 expanded configuration (upgrade)	Seven 4 TB HDDs + Five 4 TB HDDs	22 TB

Table 39. DD6300 AIO configuration

Slot 0: HDD 1	Slot 1: HDD 2	Slot 2: HDD 3	Slot 3: HDD 4
Slot 4: HDD 5	Slot 5: HDD 6	Slot 6: HDD 7	Slot 7: Filler
Slot 8: Filler	Slot 9: Filler	Slot 10: Filler	Slot 11: Filler

Table 40. DD6300 AIO expanded configuration

Slot 0: HDD 1	Slot 1: HDD 2	Slot 2: HDD 3	Slot 3: HDD 4
Slot 4: HDD 5	Slot 5: HDD 6	Slot 6: HDD 7	Slot 7: HDD 8
Slot 8: HDD 9	Slot 9: HDD 10	Slot 10: HDD 11	Slot 11: HDD 12

Front LED indicators

The front of the system contain 12 disk drive status LEDs that are normally blue, and blink when there is activity on the disk. The LEDs are shaped like triangles, and the apex of the triangle points left or right, indicating that disk's status. If the disk drive has a failure, the disk's status LED turns from blue to amber, indicating that a drive must be replaced.

The front also contains two system status LEDs. A blue system power LED is present that is on whenever the system has power. An amber system fault LED is also present that is normally off and lit amber whenever the chassis or any other FRU in the system requires service.

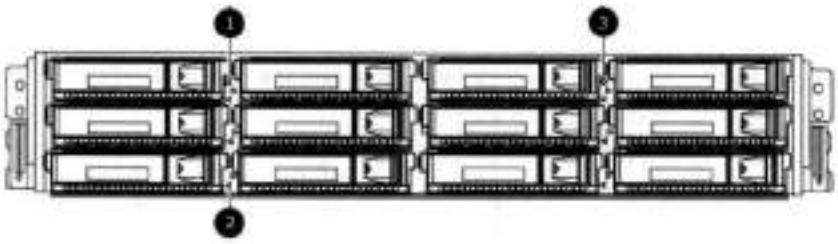


Figure 65. Front LED indicators

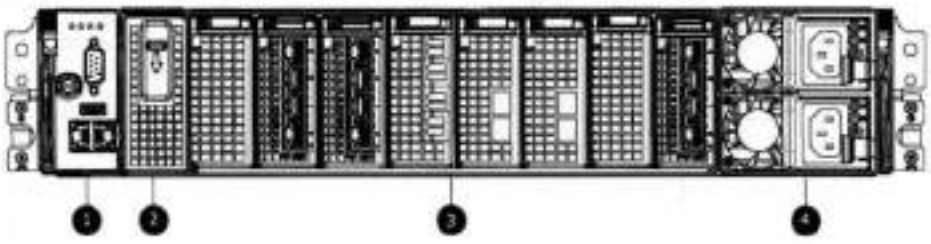
1. System service LED
2. Drive activity/service LED
3. System power LED

Table 41. Front LEDs

Name	Color	Purpose
System power LED	Blue	Indication that the system has power.
System service LED	Amber	Normally off; is lit amber whenever the SP or any other FRU (except disk drives) in the system requires service.
Drive activity/Service LED	Blue /Amber	• Lit blue when the drive is powered. • Blinks blue during drive activity. • Lit solid amber when a disk needs service.

Back panel

The back panel of the chassis contains the following components:



1. Management panel
2. Two 2.5" SSD slots labeled 0 and 1
3. I/O module slots
4. Power supply modules (PSU 0 is the lower module, and PSU 1 is the upper module)

DD6300 rear SSDs

The D6300 system uses one or two 800 GB SSDs mounted at the rear of the chassis for metadata caching:

Table 42. DD6300 rear SSDs

Configuration	Number of SSDs	SSD location
DD6300	1	SSD slot 0
DD6300 expanded	2	SSD slots 0 and 1
ⓘ **NOTE:** SSDs are not RAID-protected.		

Rear LED indicators

Figure 66. Rear LED indicators

1. Do not remove LED
2. SP service LED
3. System power LED
4. AC power good LED
5. DC power good LED
6. Power supply fault LED

Name of LED	Location	Color	Definition
"Do not remove" LED	Upper left-most part of rear chassis	White	This LED is lit during system BIOS and BMC firmware updates and indicates that the SP should not be removed from the chassis, nor should system power be removed.

Name of LED	Location	Color	Definition

SP service LED	To the right of "Do not remove" LED	Amber	• Solid amber - SP or a FRU inside the SP requires service
			• Blinking amber - blink rate reflects one of the following is booting
			  ○ BIOS - 1/4 Hz
			  ○ POST - 1 Hz
			  ○ OS - 4 Hz

Drive Power/Activity LED [a]	Left LED on the SSD	Blue	Lit blue when the drive is powered. Blinks during drive activity.
Drive Fault LED [a]	Right LED on the SSD	Amber	Lit solid amber when a drive needs service.
System power LED	Right-most LED on the management panel	Blue	SP has good, stable power
PSU FRU LED - AC Good	Top LED on power supply	Green	AC input is as expected
PSU FRU LED - DC Good	Middle LED on power supply	Green	DC output is as expected
PSU FRU LED - Attention	Bottom LED on power supply	Amber	PSU has encountered a fault condition

a. The SSD is only present on DD6300 systems.

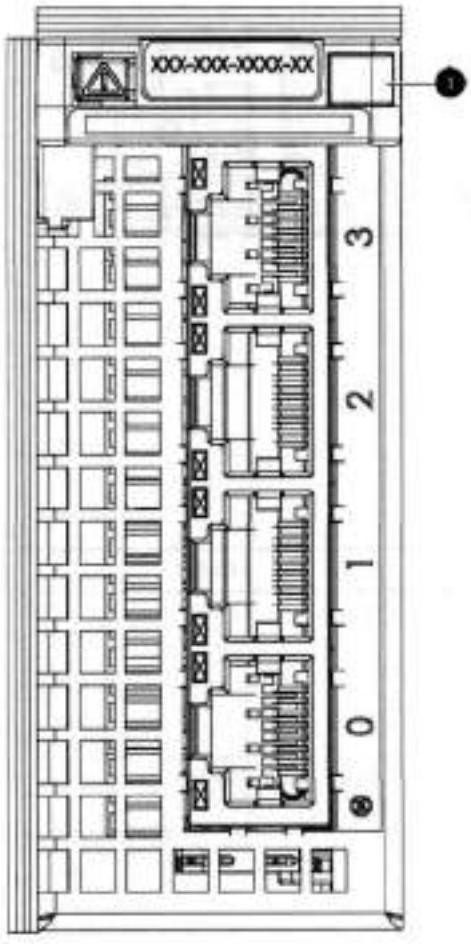


Figure 67. I/O module Power/Service LED location

1. I/O module power/service LED

Table 43. I/O LEDs

Name of LED	Location	Color	Definition
I/O module FRU LED - I/O module Power/Service LED location	Ejector handle of I/O modules	Green/Amber	• Green - I/O module has power and is functioning normally • Amber - I/O module has encountered a fault condition and requires service
I/O port status LED (SAS, Fibre Channel, and optical networking I/O modules only)	One LED per I/O module port	Blue	Lit when port is enabled. May flash if SW "marks" the port. [a]

a. For RJ45 networking ports, the standard green link and amber activity LEDs are used.

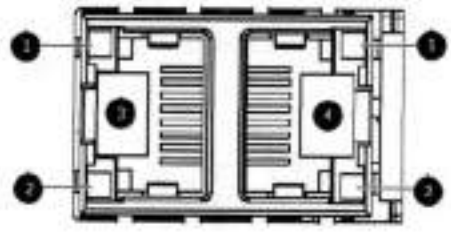


Figure 68. Onboard network port LEDs

1. Network port link LED
2. Network port activity LED
3. Dedicated IPMI port BMC0A
4. Management interface Eth/Ma

Table 44. Onboard network port LEDs

Name of LED	Location	Color	Definition
Onboard network port LED - Link LED Onboard network port LEDs	Top LED on network port	Green	• Lit when there is a link at 1000BaseT and 100BaseT speeds • Off when the link speed is 10BaseT or there is no link
Onboard network port LED - Activity LED	Bottom LED on network port	Amber	Blinks when there is traffic on the port

I/O modules

I/O module slot numbering

The eight I/O module slots are enumerated as Slot 0 (on the left when viewed from the rear) through Slot 7. Ports on an I/O module are enumerated as 0 through 3, with 0 being on the bottom.

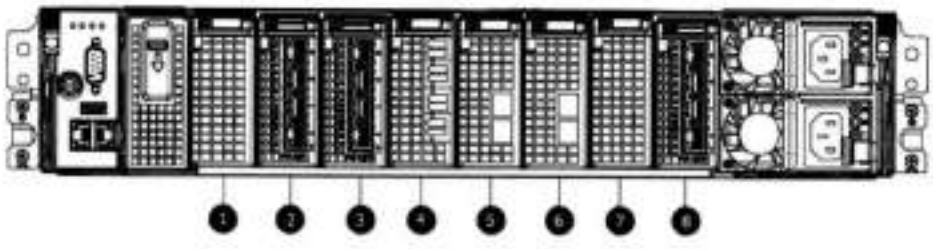


Figure 69. I/O module slot numbering

1. Slot 0
2. Slot 1
3. Slot 2
4. Slot 3
5. Slot 4
6. Slot 5
7. Slot 6
8. Slot 7

I/O modules are only supported in fixed configurations. The fixed configurations define the exact slots into which the I/O modules may be inserted. The processors directly drive the eight I/O module slots, meaning all slots are full performance.

The non-optional SAS, NVRAM, and 10GBaseT I/O modules are allocated to fixed slots. The optional Host Interface I/O modules are used for front end networking and Fibre Channel connections. The quantity and type of these I/O modules is customizable, and there are many valid configurations.

DD6300 slot map

Slot 0, Slot 1, Slot 2 (except when it is marked "Reserved") are populated with the required I/O modules and are not optional. I/O module slots 3-7 contain optional Host Interface I/O modules and can contain specific I/O modules or no I/O modules at all.

Table 45. DD6300 I/O slot module mapping

Tier	Slot 0	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7
AIO Expanded	NVRAM 8g Model 3	Quad Port 10 GBase-T	Reserved	(Optional) Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	(Optional) Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	(Optional) Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	(Optional) Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	(Optional) Quad Port 6 Gbps SAS [a]
AIO	NVRAM 8g Model 3	Quad Port 10 GBase-T	Reserved	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 6 Gbps SAS[a]

a. Optional in configurations, but required with one or more external storage shelves.

I/O module population rules

The system chassis has eight slots for I/O modules. Slots 0, 1, 2, and 7 are reserved. Slots 3, 4, 5, and 6 support host interface I/O modules. The maximum supported number of any type of host interface I/O module is four.

NOTE: A maximum of three Quad Port 10 GBase-T I/O modules are supported in slots 3-6 because of the mandatory Quad Port 10 GBase-T I/O module in slot 1.

The following table assigns rules for populating the I/O modules.

Table 46. I/O module slot population rules

Step	I/O module name	Slots	Notes
Step 1: Populate mandatory I/O modules	NVRAM 8g Model 3	0	Mandatory for all configurations
	Quad Port 10 GBase-T	1	Mandatory for all configurations
	Quad Port 6 Gbps SAS	2	Reserved for expanded configuration.
	Quad Port 6 Gbps SAS	7	Reserved for for base configuration.
Step 2: Populate all Quad Port 10GbE SR I/O modules	Quad Port 10GbE SR	3, 4, 5, 6	Populate starting from the lowest available slot number.
Step 3: Populate all Quad Port 10 GBase-T I/O modules	Quad Port 10 GBase-T	3, 4, 5, 6	Populate starting from the lowest available slot number. With Quad Port 10 GBase-T

Table 46. I/O module slot population rules (continued)

Step	I/O module name	Slots	Notes
			in slot 1, max number of Quad Port 10 GBase-T I/O modules are limited to 4.
Step 4: Populate all Dual Port 16 Gbps Fibre Channel I/O modules	Dual Port 16 Gbps Fibre Channel	6, 5, 4, 3	Populate starting from the highest available slot number.

Internal system components

The following figure shows the layout of the CPUs and DIMMs inside the chassis. The front of the system is at the top of the figure.

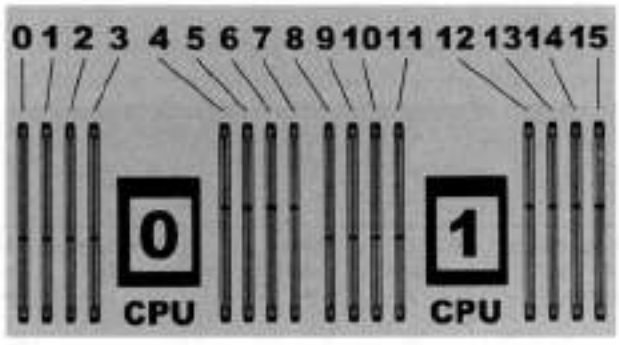


Figure 70. CPU and memory locations

DIMMs overview

Dual in-line memory modules (DIMM) come in various sizes, which must be configured in a certain way. This topic can help you select the correct configuration when servicing DIMMs.

The storage processor contains two Intel processors each with an integrated memory controller that supports four channels of memory. The storage processor allows two DIMM slots per channel, so the storage processor supports a total of 16 DIMM slots.

DD6300 memory DIMM configuration

Table 47. DD6300 memory DIMM configuration

Tier	Total Memory	Memory DIMM Configuration
AIO Expanded	96 GB	12 x 8 GB
AIO	48 GB	6 x 8 GB

To ensure maximum memory performance, there are memory DIMM population rules for best memory loading and interleaving. Memory locations - CPU 0 and Memory locations - CPU 1 specify the DIMM location rules for various memory configurations:

Table 48. Memory locations - CPU 0

		Channel A		Channel B		Channel D		Channel C	
Tier	Total Memory	0	1	2	3	4	5	6	7
AIO Expanded	96 GB	8 GB	N/A	8 GB	N/A	8 GB	8 GB	8 GB	8 GB
AIO	48 GB	N/A	N/A	8 GB	N/A	N/A	8 GB	N/A	8 GB

Table 49. Memory locations - CPU 1

		Channel A		Channel B		Channel D		Channel C	
Tier	Total Memory	8	9	10	11	12	13	14	15
AIO Expanded	96 GB	8 GB	8 GB	8 GB	8 GB	N/A	8 GB	N/A	8 GB
AIO	48 GB	8 GB	N/A	8 GB	N/A	N/A	8 GB	N/A	N/A

DD6300 and ES30 shelf guidelines

The system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your system as listed in the following table below.
- Use the Installation and Setup Guide for your system to minimize the chance of a cabling mistake.
- A system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.
- ES30 SATA shelves must be on their own chain.

Table 50. DD6300 and ES30 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	ES30 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB) [1]	Max RAW external capacity (TB) [2]
DD6300	48	1x4 (Optional)	SAS 30, 45, 60	1	1	49	60
DD6300 w/ Expanded Capacity [3]	96	1x4 (Optional)	SAS 30, 45, 60	5	1	144	180

1. This figure only counts drives that have user data in the shelves.

2. The raw capacity of an ES30 is 125% of the available capacity.

3. DDOS 6.0 and FS15 SSD shelf configuration

Types of cabinets and power connections

The ES30 chassis is installed in two types of racks: 40U-C (existing racks) and the 40U-P (newer racks). The racks use one phase or 3-phase power connections.

3-Phase power connections for 40U-P (current racks)

Some environments use 3-phase power for 40U-P racks that are used for several systems. In those situations, it is desirable to balance the current draw across all three phases. The recommended 3-phase power cabling attempts to do that, but an optimal configuration depends on the specific installation.

Cabling shelves

NOTE:

- Before cabling the shelves, physically install all shelves in the racks. Refer to the rail kit installation instructions included with the ES30 shelf for rack mounting.
- The documentation refers to two SAS HBAs. If only one HBA is allowed in a system, then use another port as defined later for that specific system.
- On an HA system, add cables from the second node to open ports at the end of the sets. The ports on the second node must connect to the same sets as the corresponding ports on the first node.

Ports on the system's SAS HBA cards connect directly to a shelf controller's host port. For redundancy, you need to create dual paths by using a port on one SAS HBA card to connect to one shelf controller in each shelf set, and a port on another SAS HBA card to connect to another shelf controller in the same shelf set. With dual paths, if one SAS HBA card fails, the shelf is still operational. However, in the unlikely event any single shelf becomes completely disconnected from power or SAS cables and becomes disconnected from a previously operational shelf, the file system goes down and the shelf is not operational. This is considered a double failure.

There are two kinds of configurations: one shelf in a set or multiple shelves in a set.

DD6300, DD6800, and DD9300 shelf configurations

There are a few rules that must be followed when adding a mixture of DS60 and other shelf types to your system.

CAUTION: **If a system does not follow ALL of these rules it is not a legitimate configuration.**

Prerequisites:

- You cannot exceed the maximum amount of raw capacity displayed in the cabling table for each system.
- You cannot exceed the maximum number of shelves displayed in the cabling table for each system.
- There are no specific placement or cabling requirements for SSD shelves, or the metadata shelves for Cloud Tier configurations. These shelves can be installed and cabled the same way as standard ES30 shelves.

Table 51. Minimum and maximum configurations

System	Appliance	Minimum appliance shelf count*	Max appliance shelf count
	48 TB usable	0	1
w/ Expansion	144 TB usable	1	5
	144 TB usable	2	28
w/ Expansion	288 TB usable	2	28
w/ High Availability (HA)	288 TB usable	2	28
w/ Extended Retention (ER)	576 TB usable	2	28
w/ Cloud Tier	288 TB usable (96 TB for Cloud Tier)	2	28
w/ HA and Cloud Tier	288 TB usable (96 TB for Cloud Tier)	2	28
	384 TB usable	3	28
w/ Expansion	720 TB usable	3	28
w/ HA	720 TB usable	3	28
w/ ER	1440 TB usable	7	28
w/ Cloud Tier	720 TB usable (192 TB for Cloud Tier)	7	28
w/ HA and Cloud Tier	720 TB usable (192 TB for Cloud Tier)	7	28

* The minimum appliance shelf count does not include shelves for Cloud Tier.

DD6300 and DS60 shelf guidelines

The system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your system as listed in the following table.
- For redundancy, the two connections from a system to a set of shelves must use ports on different SAS I/O modules.
- Use the Installation and Setup Guide for your system to minimize the chance of a cabling mistake.
- A system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.
- ES30 SATA shelves must be on their own chain.
- If ES30 SAS shelves are on the same chain as a DS60, the maximum number of shelves on that chain is 5.

Table 52. DD6300 and DS60 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	DS60 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB)[1]	Max RAW external capacity (TB)
DD6300 [2]	48 [3]	1x4 [4]	N/A	0	0	48	60
DD6300 w/ Expanded Capacity [2]	96	1x4 [4]	SAS 45, 60 [5]	1	1	144	180

NOTE: An entry of 45 corresponds to DS60-3 models and an entry of 60 corresponds to DS60-4 models.

1. This column only counts drives that have user data in the shelves. For example, a DS60 4-240 has 192TB.

2. Only available with DD OS 6.x and greater.

3. Base configuration does not support DS60 additional capacity; must have memory configuration of 96GB.

4. One SAS card is optional and must be ordered with external SAS shelf order. Dual paths from the single SAS card to external shelves are required.

5. The DS60 will have a maximum of 45 4Tb drives.

shelf configurations

There are a few rules that must be followed when adding a mixture of DS60 and other shelf types to your system.

CAUTION: **If a system does not follow all these rules, it is not a legitimate configuration.**

Prerequisites:

- You cannot exceed the maximum amount of raw capacity displayed in cabling table for each system.
- You cannot exceed the maximum number of shelves displayed in cabling table for each system.
- You cannot connect more than three DS60 shelves in a single set.

Table 53. Minimum configurations

System	Appliance maximum	Minimum appliance DS60 shelf count
	144 TB	0
	144 TB	2
w/ High Availability (HA)	288 TB	2 (plus 1 FS15 for SSD cache)
w/ Extended Retention (ER)	576 TB	2
w/ Cloud Tier	384 TB (96 TB for Cloud Tier)	2 (plus 2 ES30s for Cloud Tier)
w/ HA and Cloud Tier	384 TB (96 TB for Cloud Tier)	2 (plus 1 FS15 for SSD cache, and 2 ES30s for Cloud Tier)
	384 TB	3
w/ HA	720 TB	3 (plus 1 FS15 for SSD cache)
w/ ER	1440 TB	3
w/ Cloud Tier	912 TB (192 TB for Cloud Tier)	3 (plus 4 ES30s or 1 DS60 for Cloud Tier)
w/ HA and Cloud Tier	912 TB (192 TB for Cloud Tier)	4 (plus 1 FS15 for SSD cache, and 4 ES30s or 1 DS60 for Cloud Tier)

1. DS60 will only be partially filled.

- A Cloud Tier system shares the ERSO cabling configuration; however, Cloud Tier has a lower maximum.
- It is recommended that the shelf with the greater number of drives should always be placed in the bottom position.
- only supports one DS60.
- only has one SAS SLIC and all DS60 connections are made to that single SAS SLIC.

- only has one SAS SLIC and all DS60 connections are made to that single SAS SLIC.

6

DD6400

Topics:

- DD6400 system features
- DD6400 system specifications
- Front LED indicators
- Rear LEDs
- Storage configurations
- DD6400 I/O modules
- DD6400 cabling

DD6400 system features

Table 54. DD6400 system features

Feature			Single Node
Processor			2 x Intel Xeon Silver, 2.2 Ghz, 10C/20T
Kernel			4.4
Memory Configurations	Total		192 GB
	DIMMs		12 x 16 GB
HDD Drive Size			8 TB
Supported Capacity	Active Tier	Base	12 <-> 32 TBu
		Expanded	36 <-> 172 TBu
	Cloud Tier	Base	64 TBu
		Expanded	344 TBu
SSDs for DD OS in 2.5"			2, 0.96 TB, 1 WPD
Stream Count			270 Wr, 75 Rd
Cache SSDs	Base (6% of 32 TBu)		1 (Internal) 1.92 TB
	Expanded (2.2% of 172 TBU)		2 (Internal) 1.92 TB
16 GB NVRAM			1
HW Accelerator	Quick Assist Technology (QAT) 8970		1
Internal SAS	HBA330 12 Gbps SAS controller		1
External SAS	Dual Port 12 Gbps SAS		1
SAS String Depth (max)	ES40		2
Host Interface	2-port 25 GbE-SFP28		3 maximum
	4-port 10 GbE-SFP+		3 maximum
	4-port 10GBASE-T		3 maximum

Table 54. DD6400 system features (continued)

Feature		Single Node
	4-port 16 Gb FC	1 maximum
Network Daughter Card option (system will have one of the two options)	4-port 10 GbE-SFP+	1
	4-port 10GBASE-T	1

DD6400 system specifications

Table 55. DD6400 system specifications

Average power consumption 25 C	Heat dissipation (operating maximum)	Weight [a]	Width	Depth	Height
530W	1.69 x 10^6 J/hr (1604 Btu/hr) maximum	80 lbs (36.29 kg)	17.50 in (44.45 cm)	30.5 in (77.5 cm)	3.40 in (8.64 cm)

a. The weight does not include mounting rails. Allow 2.3-4.5 kg (5-10 lb) for a rail set.

Temperature	Specification
Standard Environment	
Storage	-40C to 65C (-40F - 149F)
Continuous operation (for altitude less than 950m or 3117 ft)	10C to 35C (50F to 95F) with no direct sunlight on the equipment
Maximum temperature gradient (operating and storage)	20C/h (68F/h)
Expanded Operating Temperature (Fresh Air)	
Continuous operation	5C to 40C at 5% to 85% RH with 29C dew point **NOTE:** Outside the standard operating temperature (10C to 35C), the system can operate continuously in temperature as low as 5C and as high as 40C. For temperature between 35C to 40C, derate maximum allowable temperature by 1C per 175m above 950m (1F per 319 ft)
≤ 1% of annual operating hours	-5C to 45C at 5% to 90% RH with 29C dew point **NOTE:** Outside the standard operating temperature (10C to 35C), the system can operate down to -5C or up to 45C for a maximum of 1% of its annual operating hours. For temperature between 40C to 45C, derate maximum allowable temperature by 1C per 125m above 950m (1F per 228 ft)

NOTE: When operating in the expanded temperature range, system performance may be impacted.

Front LED indicators

DD6400 contains many LEDs. This section details their location and function.

Table 56. Front LEDs

Name	Color	Purpose
Control Panel Status LED	Blue/ Amber	Status • Healthy: Solid Blue • Fault: Blink Amber • Sys ID: Blink Blue
System Power Button and LED	Green	Indication that the system has power.
Drive Activity LEDs	Green	Lit green when the drive is powered and blinks during drive activity.
Drive Service LEDs	Green	Lit solid amber when a disk drive needs service.

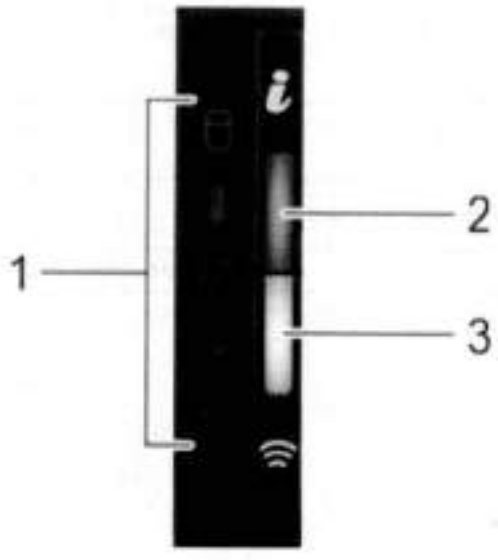


Figure 71. DD6400 Front Left Control Panel Status LEDs

1. Status LED indicators
2. System health and system ID indicator
3. iDRAC Quick Sync 2 wireless indicator (not used)

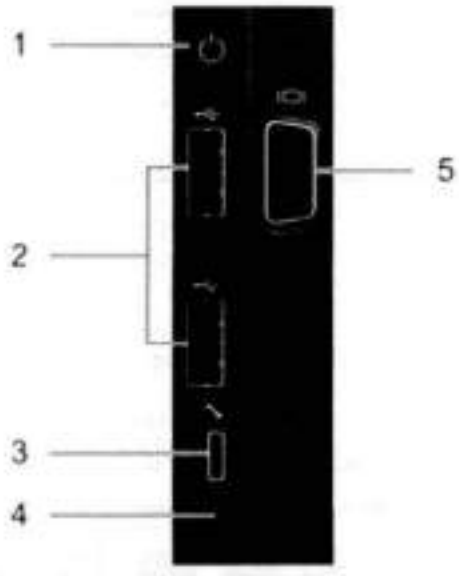


Figure 72. DD6400 Front Right Control Panel Power Button and LEDs

1. Power
2. USB port (2)
3. iDRAC Direct port
4. iDRAC Direct LED
5. VGA port

Figure 73. Drive LEDs

The front of the DD6400 contains 3.5" disk drive slots that can be populated with HDDs or SSDs. Each is housed in a drive carrier that contains two LEDs/indicators. One LED indicates the power. The other indicates the activity when blinking. (See the *Dell EMC PowerProtect DD6400 Installation Guide* for more details.)

Rear LEDs

PSU LEDs

Each power supply has a status LED which illuminates the PSU handle. The following table shows the status LED behavior.

Table 57. PSU LEDs

Name	Color	Definition
Good	Solid Green	Working normal
Service	Blinking Amber	PSU has a fault condition and must be replaced.

ID and iDRAC LEDs

The iDRAC management port:

- The green link LED on the left is lit whenever there is link at 1000BaseT and 100BaseT speeds. The link LED is off when the link speed is 10BaseT or there is no link.
- The green link LED on the right blinks whenever there is traffic on the port.

System identification LED: This blue LED can be turned on by software to visually identify the system.

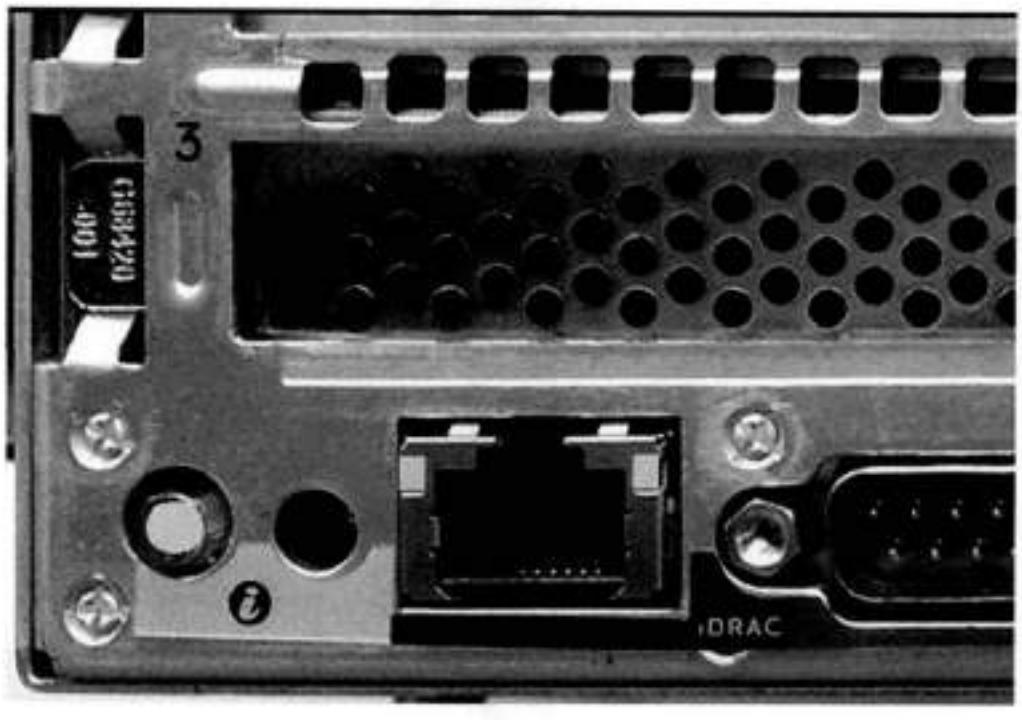


Figure 74. Onboard ID and iDRAC LEDs

Storage configurations

The system uses three classes of storage: Boot, Cache, and Storage (active tier and cloud tier). The DD6400 head unit drive usage is defined in the following table:

Table 58. DD6400 head unit drive usage

Use	Type	Positions
Boot/OS	960 GB SAS SSD	00, 01
Cache1	1.92 TB SAS SSD	02
Cache2 (expansion)	1.92 TB SAS SSD	03
Data (FS)	8 TB SAS HDD	04-11

Boot drives

The DD6400 uses two internal SAS SSDs to boot and for the operating system. Boot disks and external storage shelves are used to log system information.

Cache SSD

The DD6400 system requires a certain minimum number of disk drive read I/O operations per second per second (IOPs) in order to properly maintain rated backup throughput performance. Due to the increase of disk drive capacities, large system storage capacities can be created that do not provide enough IOPs since there are fewer disks operating in parallel. SSDs are used to overcome the lack of read IOPs using larger disk drives as a metadata cache to provide the required read IOPs to that metadata.

Table 59. DD6400 SSD characteristics

	Writes Per Day	Read IOPs	Sequential Read Throughput	Random Write Throughput
External Capacity SSD	1 WPD	102K@4K	409 MB/s	30 MB/s

External storage shelves

DD6400 systems store data on internal disk drives. In addition, external disk array shelves provide optional additional storage. ES40 shelves (with 8 TB drives) are connected to the DD6400 systems using 12 Gb Mini-SAS HD ports which are implemented on the SAS HBAs.

Storage shelves and usable storage capacity

The ES40 SAS shelf contains 15 x 8 TB drives, two of which are parity drives and one is a hot spare, so each ES40 shelf provides 12 drives of usable storage. The rough estimate of usable capacity of each shelf is 76 TB of usable capacity, which means that two shelves plus the base would support approximately 184 TB and the associated CT metadata capacity. Only 172 TB is presented. If necessary, either a smaller maximum can be supported to meet performance requirements or an additional shelf can be added.

The table below shows capacity for each physical increment.

Hard drive size (TB)	Shelf
8	ES40-120T

Table 60. DD6400 capacities

Configuration	Supported capacity
Base (8 internal 8 TB drives)	32 TB
Base and one ES40	104 TB
Base and two ES40s	172 TB

Each SAS chain is a dual-path SAS connection requiring two Mini-SAS HD connections, which protects against ES40 controller failures and improves reliability. Only a single, 2-port, SAS controller is used. One port is connected to LCC-A and the other is connected to LCC-B.

NOTE: While the system is designed to use only two shelves, there are no checks or alerts if more than two shelves are added.

DD6400 I/O modules

The DD6400 contains three types of I/O:

- Onboard

- rNDC
- HBA I/O

There are four predefined locations for I/O cards: NVRAM, QAT, Internal SAS, and the 2-port External SAS card. The rNDC can be either a 4-port 10GbT or 4-port 10Gb-SFP+.

Onboard I/O

Onboard I/O includes:

1. One 1000Base-T system management port. This is a BMC LAN connection that is used for serial-over-LAN or for direct BMC interaction such as remote iDRAC access (above the two USB ports).
2. One DB-9 serial port on the back.
3. One VGA port in back. This connector is covered on production systems.
4. Two USB 3.0 type A in back. Used for USB drive based DDOS upgrade.

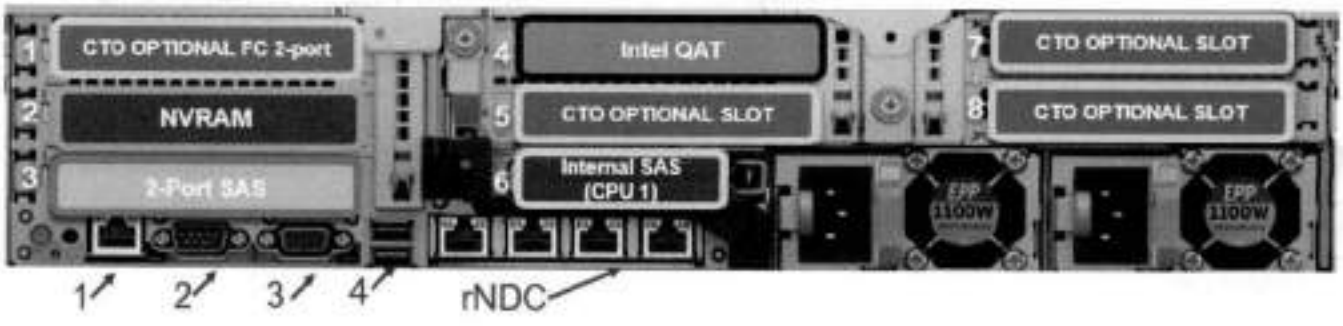


Figure 75.

- One micro USB 2.0 iDRAC direct port in front
- One USB 2.0 type A in front.

rNDC

The rNDC slot is always included, but there is the option to use a 4-port 10Gbe-T (copper) or 4-port 10Gbe-SFP+ (optical).

HBAs

The DD6400 uses the standard form factor PCIe HBAs. Both network and SAS HBAs provide host and disk shelf interface options for the systems. All HBAs share common design features:

- PCI Express gen 3, x8 or x16 compatible.
- VPD data available through the iDRAC or in-band PCIe.
- Power consumption 25 W max.

An empty PCIe slot must install a blank bracket. This is required for EMI compliance and appropriate thermal air flow.

PCIe Slot 1 is FH x8 and will be dedicated to a Fibre Channel card if it is included.

PCIe Slot 2 is FH x8 and is dedicated for the NVRAM card.

PCIe Slot 3 is FH x8 and is dedicated for the external 2-port SAS card.

PCIe Slot 4 is FH x16 and is dedicated for the Intel QAT card.

PCIe Slot 5 is FH x8 and is available for optional NIC cards

PCIe Slot 6 is LP x8 and is dedicated for the INTERNAL SAS card.

PCIe Slot 7 is FH x8 and is available for optional NIC cards.

PCIe Slot 8 is FH x16 and is available for optional NIC cards.

Supported I/O Cards Map

The following table lists the PCIe cards and the slot priority matrix for the DD6400. The lower priority number determines the first card installed. Cards that have the same priority are considered equivalent.

Form Factor	Vendor/PN	Description	DPN	Priority	Slots
rNDC	Intel X710	4 x 10 GbE SFP+	68M85	1	rNDC
rNDC	QLogic 41164	4 x 10 GbE SFP+	XVVY1	1	rNDC
rNDC	Intel X550	4 x 10GBT	64PJ8	1	rNDC
rNDC	QLogic 41164	4 x 10GBT	X1TD1	1	rNDC
PCIe FH	Intel XXV710	2 x 10/25GbE SFP28	HN7J7	7	5,8,7
PCIe FH	Broadcom 57414	2 x 10/25GbE SFP28	CX94X	7	5,8,7
PCIe FH	Intel X710	4 x 10 GbE SFP+	DDJKY	8	5,8,7
PCIe FH	QLogic 41164	4 x 10 GbE SFP+	0HY9T	8	5,8,7
PCIe FH	Intel X710	4 x 10GBT	K5V44	9	5,8,7
PCIe FH	QLogic 41164	4 x 10GBT	33M0K	9	5,8,7
PCIe FH	Broadcom LSI 9300-8e	2 x SAS 12 Gbps (external)	6PDH5	3	3
PCIe FH	QLogic 2692	2 x 16G FC	YCVFG	4	1
PCIe FH	Dell EMC Cavium/ CN72xx	NVRAM	DGK85	2	2
PCIe FH	Intel Lewisberg	QAT	93XWF	5	4
PCIe LP	Broadcom LSI 9300-8e	2 x SAS 12 Gbps (internal)	405-AANK	6	6

DD6400 cabling

Management cabling

The DD6400 provides two methods to access the system console: a dedicated iDRAC management 10/100/1000Base-T port and an RS-232 serial RJ-45 port. Both are at the rear of the enclosure.

Management Ethernet Cabling

A minimum of TIA or EIA 568-B Cat5 twisted-pair copper cables with RJ-45 jacks up to 100 m in length can be plugged into the management 10/100/1000GbE port. Cat 5E, Cat 6, and Cat6A cables, up to 100 m in length may also be used.

Management Serial Console Cabling

Serial over LAN or RJ-45 connector provides the serial console for the system. A null modem adapter is used. The system serial console is configured for a terminal type of VT100+, 115200 baud, 8 data bits, no parity, 1 stop bit, and no flow control.

Host interface cabling

LOM

The DD6400 LOM card (DPN) provides two 10GBase-T Host Interface ports. RJ-45 connectors provide the interface to the 10GBase-T copper cables. The 10GBase-T ports support 100 m cable length with category 6 cable or 55 m with category 6 cable.

The alternate LOM (DPN) provides 1 20G SFP+ ports. The SFP+ connectors should be populated with 850 nm 10 GbE Optical Transceivers supporting the 10GBASE-SR standard (DPN or equivalent).

10GBase-T HBA

This set of 4-port HBAs (DPNs) supports the same cable as 10GBase-T LOM.

10GbE/25GbE Optical Ethernet HBA

The SFP28 connectors on the (DPNs) 25 GbE dual port cards are populated with 850 nm 10GbE/25GbE Optical Transceivers supporting both the 10GBASE-SR and the 25GBASE-SR standard (DPN M14MK).

10 GbE Ethernet HBA

The SFP+ connectors on the (DPNs) 10 GbE dual port are populated with 850 nm 10 GbE Optical Transceivers supporting the 10GBASE-SR standard (DPN C5RNH).

Supported optical fiber cable lengths depend on the type of optical fiber that is connected to the SFP+ Optical Transceivers. The following table summarizes the supported 10GBASE-SR lengths that are provided by the SFP+ transceiver:

Table 61. Optical cable max cable length @ 10 Gb

Fiber Type	Minimum modal bandwidth @ 850 nm (MHz*km)	Operating range (meters)
62.5 µm MMF (OM1)	160	2–26
62.5 µm MMF (OM1)	200	2–33
50 µm MMF (OM2)	400	2–66
50 µm MMF (OM2)	500	2–82
50 µm MMF (OM3)	1500	2–300
50 µm MMF (OM4)	3500	2–400

16 Gbps Fibre Channel HBA

The FibreChannel HBA provides two 16Gbps Fibre Channel ports. The card contains two SFP+ ports that accommodate 16 Gb SFP+ Optical Transceivers.

The SFP+ connectors on the HBA are pre-populated with QLogic certified 850 nm 16 Gb Fibre Channel Optical SFPs.

The maximum supported cable distance depends on both the data rate and optical cable type (OM1, OM2 or OM3). The following table summarizes the maximum supported cable lengths:

Table 62. Fibre Channel data rate and cable length limits

Data Rate	Multi-Mode Optical Cable Type		
	OM1	OM2	OM3
4 Gb FC	70 m	150 m	380 m

Table 62. Fibre Channel data rate and cable length limits (continued)

Data Rate	Multi-Mode Optical Cable Type		
	OM1	OM2	OM3
8 Gb FC	21 m	50 m	150 m
16 Gb FC	15 m	35 m	100 m

SAS cabling

The 15-disk drive array enclosure ES40 is supported with DD6400 systems. The mini-SAS-HD cable is used to connect a DD6400 system with ES40 enclosure. There is no special keying feature to differentiate connections between the first node or the second node in an A-P HA configuration. Typical cable length and their part numbers are listed below.

ES40 shelves come with a 1M Mini-SAS-HD to Mini-SAS-HD cable. That length is enough for most installations. The cables that are listed in the table can be used but must be ordered.

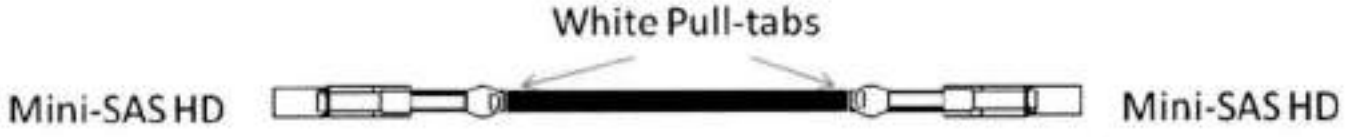


Figure 76. SAS Card to ES40 SAS Cable

Table 63. DD6400 to ES40 shelf SAS cables

Description	Part number
1M 12G MINI-HDX4 TO MINI-HDX4 HAL-FREE	038-004-448-00
2M 12G MINI-HDX4 TO MINI-HDX4 HAL-FREE	038-004-449-00
3M 12G MINI-HDX4 TO MINI-HDX4 HAL_FREE	038-004-450-00
5M 12G MINI-HDX4 TO MINI-HDX4 CABLE	038-004-382-01

7

DD6800

This chapter contains the following topics:

Topics:

- DD6800 system features
- DD6800 system specifications
- DD6800 storage capacity
- DD6800 front panel
- Back panel
- I/O modules
- Internal system components
- DD6800 and ES30 shelf guidelines
- DD6800 and DS60 shelf guidelines

DD6800 system features

Table 64. DD6800 system features

Feature		Base configuration	Expanded configuration
Rack height		2U	2U
Processor		E5-2630 V3	E5-2630 V3
Kernel		3.2.x	3.2.x
NVRAM		NVRAM 8g Model 3	NVRAM 8g Model 3
Memory		8 x 8 GB DIMM + 8 x 16 GB DIMM (192 GB)	8 x 8 GB DIMM + 8 x 16 GB DIMM (192 GB)
Internal drives	HDDs in 3.5" bays	7/ 7+5	12
	SSDs in 3.5" bays	0	0
	SSDs in 2.5" bays	1	2
I/O module slots	SAS I/O modules (Quad Port 6 Gbps SAS)	2	2
	Network and FC I/O modules	Four replaceable I/O module slots. Not hot-swappable.	Four replaceable I/O module slots. Not hot-swappable.
Supported capacity	Non-extended retention	144 TB	288 TB
	DD Cloud Tier	N/A	576 TB [a]
	Extended retention	N/A	288 TB[b]
High availability support		Yes	Yes
HA private interconnect		(2) 10GBase-T ports	(2) 10GBase-T ports
External SSD shelf		One SSD shelf for A-P high availability cluster containing two drives.	One SSD shelf for A-P high availability cluster containing four drives.
SAS string depth (max)	ES30	1	4

Table 64. DD6800 system features (continued)

Feature		Base configuration	Expanded configuration
	DS60	0	1
	ES30 and DS60	5 shelves total	5 shelves total
Stream count		405 writes, 112 reads	405 writes, 112 reads

a. DD Cloud Tier requires two ES30 shelves fully populated with 4 TB drives to store DD Cloud Tier metadata.
b. Extended retention not available on HA configurations

DD6800 system specifications

Table 65. DD6800 system specifications

Average power consumption 25 C	Heat dissipation (operating maximum)	Weight [a]	Width	Depth	Height
560W	1.69 x 10^6 J/hr (1604 Btu/hr) maximum	68 lbs (30.84 kg)	17.50 in (44.45 cm)	30.5 in (77.5 cm)	3.40 in (8.64 cm)

a. The weight does not include mounting rails. Allow 2.3-4.5 kg (5-10 lb) for a rail set.

Table 66. System operating environment

Requirement	Description
Ambient temperature	10°C - 35°C; derate 1.1°C per 1,000 ft (304 m)
Relative humidity (extremes)	20–80% noncondensing
Elevation	0 - 7,500ft (0 - 2,268m)
Operating acoustic noise	L_{wad} sound power, 7.5 Bels

DD6800 storage capacity

The following table provides storage capacity information for the DD6800 system.

Table 67. DD6800 storage capacity

Memory	Internal disks (system disks only)	External storage (raw)	Usable data storage space (TB/TiB/GB/GiB)[a]			
192 GB (Base)	• 4 x 4 TB HDD • 2 x 800 GB SSD	180 TB[b]	144 TB	131 TiB	144,000 GB	134,110 GiB
192 GB (Expanded)	• 4 x 4 TB HDD • 4 x 800 GB SSD	• Active Tier: 360 TB[b] • Archive Tier: 360 TB[c] • Cloud Tier: 720 TB in the cloud[d] • Cloud Tier metadata: 120 TB	• Active Tier: 288 TB • Archive Tier: 288 TB • Cloud Tier: 576 TB • Cloud Tier metadata: 96 TB	• Active Tier: 261.9 TiB • Archive Tier: 261.9 TiB • Cloud Tier: 523.8 TiB • Cloud Tier metadata: 87.3 TiB	• Active Tier: 288,000 GB • Archive Tier: 288,000 GB • Cloud Tier: 576,000 GB • Cloud Tier metadata: 96,000 GB	• Active Tier: 268,221 GiB • Archive Tier: 268,221 GiB • Cloud Tier: 536,442 GiB • Cloud Tier metadata: 89,407 GiB

Table 67. DD6800 storage capacity (continued)

Memory	Internal disks (system disks only)	External storage (raw)	Usable data storage space (TB/TiB/GB/GiB)[a]			
		local storage				

a. The capacity differs depending on the size of the external storage shelves used. This data based on ES30 shelves.
b. HA is supported.
c. HA is not supported with Extended Retention.
d. HA is supported in combination with Cloud Tier.

DD6800 front panel

DD6800 Dataless Head (DLH) systems have one of the following front panel drive configurations to host the DD OS boot drives and provide metadata caching on SSD:

Table 68. DD6800 DLH SSD requirements

Configuration	Number of SSDs
DD6800	2
DD6800 expanded	4
NOTE: SSDs are not RAID-protected.	

Table 69. DD6800 DLH configuration drive layout

Slot 0: HDD 1	Slot 1: HDD 2	Slot 2: HDD 3	Slot 3: HDD 4
Slot 4: SSD 1	Slot 5: SSD 2	Slot 6: Filler	Slot 7: Filler
Slot 8: Filler	Slot 9: Filler	Slot 10: Filler	Slot 11: Filler

Table 70. DD6800 DLH expanded configuration drive layout

Slot 0: HDD 1	Slot 1: HDD 2	Slot 2: HDD 3	Slot 3: HDD 4
Slot 4: SSD 1	Slot 5: SSD 2	Slot 6: SSD 3	Slot 7: SSD 4
Slot 8: Filler	Slot 9: Filler	Slot 10: Filler	Slot 11: Filler

Front LED indicators

The front of the system contain 12 disk drive status LEDs that are normally blue, and blink when there is activity on the disk. The LEDs are shaped like triangles, and the apex of the triangle points left or right, indicating that disk's status. If the disk drive has a failure, the disk's status LED turns from blue to amber, indicating that a drive must be replaced.

The front also contains two system status LEDs. A blue system power LED is present that is on whenever the system has power. An amber system fault LED is also present that is normally off and lit amber whenever the chassis or any other FRU in the system requires service.

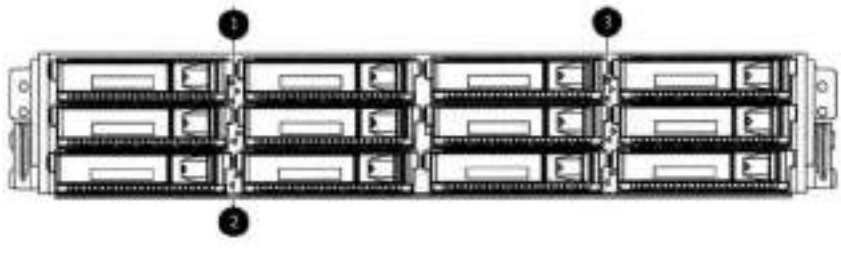


Figure 77. Front LED indicators

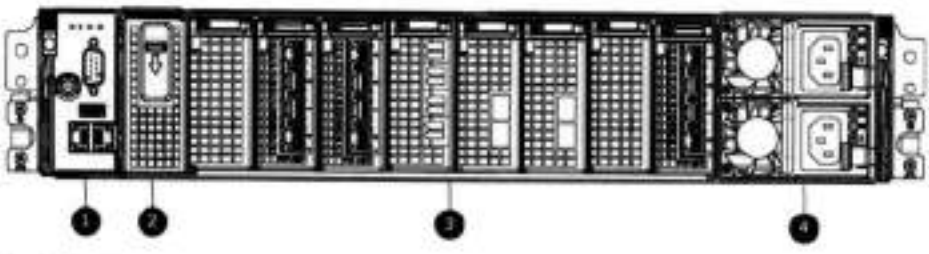
1. System service LED
2. Drive activity/service LED
3. System power LED

Table 71. Front LEDs

Name	Color	Purpose
System power LED	Blue	Indication that the system has power.
System service LED	Amber	Normally off; is lit amber whenever the SP or any other FRU (except disk drives) in the system requires service.
Drive activity/Service LED	Blue /Amber	• Lit blue when the drive is powered. • Blinks blue during drive activity. • Lit solid amber when a disk needs service.

Back panel

The back panel of the chassis contains the following components:



1. Management panel
2. Not Used -- Two 2.5" SSD slots labeled 0 and 1
3. I/O module slots
4. Power supply modules (PSU 0 is the lower module, and PSU 1 is the upper module)

Rear LED indicators

Figure 78. Rear LED indicators

1. Do not remove LED
2. SP service LED
3. System power LED
4. AC power good LED
5. DC power good LED
6. Power supply fault LED

Name of LED	Location	Color	Definition
"Do not remove" LED	Upper left-most part of rear chassis	White	This LED is lit during system BIOS and BMC firmware updates and indicates that the SP should not be removed from the chassis, nor should system power be removed.
SP service LED	To the right of "Do not remove" LED	Amber	• Solid amber - SP or a FRU inside the SP requires service • Blinking amber - blink rate reflects one of the following is booting o BIOS - 1/4 Hz o POST - 1 Hz o OS - 4 Hz
Drive Power/Activity LED [a]	Left LED on the SSD	Blue	Lit blue when the drive is powered. Blinks during drive activity.

Name of LED	Location	Color	Definition
Drive Fault LED [a]	Right LED on the SSD	Amber	Lit solid amber when a drive needs service.
System power LED	Right-most LED on the management panel	Blue	SP has good, stable power
PSU FRU LED - AC Good	Top LED on power supply	Green	AC input is as expected
PSU FRU LED - DC Good	Middle LED on power supply	Green	DC output is as expected
PSU FRU LED - Attention	Bottom LED on power supply	Amber	PSU has encountered a fault condition

a. The SSD is only present on DD6300 systems.

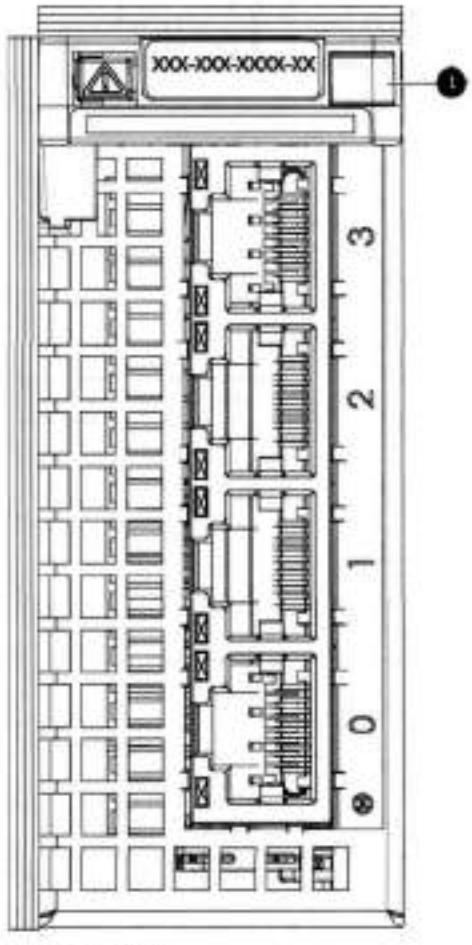


Figure 79. I/O module Power/Service LED location

1. I/O module power/service LED

Table 72. I/O LEDs

Name of LED	Location	Color	Definition
I/O module FRU LED - I/O module Power/Service LED location	Ejector handle of I/O modules	Green/Amber	• Green - I/O module has power and is functioning normally • Amber - I/O module has encountered a fault condition and requires service

Table 72. I/O LEDs (continued)

Name of LED	Location	Color	Definition
I/O port status LED (SAS, Fibre Channel, and optical networking I/O modules only)	One LED per I/O module port	Blue	Lit when port is enabled. May flash if SW "marks" the port. [a]

a. For RJ45 networking ports, the standard green link and amber activity LEDs are used.

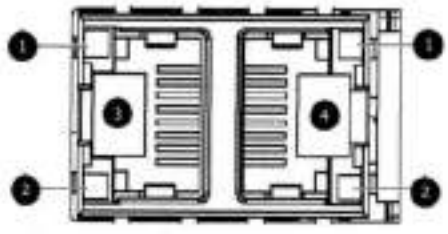


Figure 80. Onboard network port LEDs

1. Network port link LED
2. Network port activity LED
3. Dedicated iPMI port BMC0A
4. Management interface Eth/Ma

Table 73. Onboard network port LEDs

Name of LED	Location	Color	Definition
Onboard network port LED - Link LED Onboard network port LEDs	Top LED on network port	Green	• Lit when there is a link at 1000BaseT and 100BaseT speeds • Off when the link speed is 10BaseT or there is no link
Onboard network port LED - Activity LED	Bottom LED on network port	Amber	Blinks when there is traffic on the port

I/O modules

I/O module slot numbering

The eight I/O module slots are enumerated as Slot 0 (on the left when viewed from the rear) through Slot 7. Ports on an I/O module are enumerated as 0 through 3, with 0 being on the bottom.

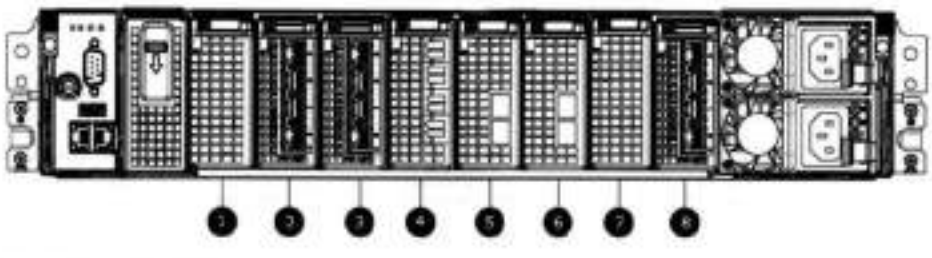


Figure 81. I/O module slot numbering

1. Slot 0
2. Slot 1
3. Slot 2

4. Slot 3
5. Slot 4
6. Slot 5
7. Slot 6
8. Slot 7

I/O modules are only supported in fixed configurations. The fixed configurations define the exact slots into which the I/O modules may be inserted. The processors directly drive the eight I/O module slots, meaning all slots are full performance.

The non-optional SAS, NVRAM, and 10GBaseT I/O modules are allocated to fixed slots. The optional Host Interface I/O modules are used for front end networking and Fibre Channel connections. The quantity and type of these I/O modules is customizable, and there are many valid configurations.

slot map

I/O module slots 3–6 contain optional Host Interface I/O modules and can contain specific I/O modules or no I/O modules at all. Slot 0, Slot 1, Slot 2, and Slot 7 are populated with the required I/O modules and are not optional.

Table 74. I/O module slot mapping

Tier	Slot 0	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7
DLH DLH Extended Retention/DD Cloud Tier	NVRAM 8g Model 3	Quad Port 10 GBase-T	Quad Port 6 Gbps SAS	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 6 Gbps SAS
DLH High Availability	NVRAM 8g Model 3	Quad Port 10 GBase-T for HA interconnect	Quad Port 6 Gbps SAS	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 6 Gbps SAS

I/O module population rules

The system chassis has eight slots for I/O modules. Slots 0, 1, 2, and 7 are reserved. Slots 3, 4, 5, and 6 support host interface I/O modules. The maximum supported number of any type of host interface I/O module is four.

NOTE: A maximum of three Quad Port 10 GBase-T I/O modules are supported in slots 3-6 because of the mandatory Quad Port 10 GBase-T I/O module in slot 1.

The following table assigns rules for populating the I/O modules.

Table 75. I/O module slot population rules

Step	I/O module name	Slots	Notes
Step 1: Populate mandatory I/O modules	NVRAM 8g Model 3	0	Mandatory for all configurations
	Quad Port 10 GBase-T	1	Mandatory for all configurations
	Quad Port 6 Gbps SAS	2	Mandatory for all configurations
	Quad Port 6 Gbps SAS	7	Mandatory for all configurations

Table 75. I/O module slot population rules (continued)

Step	I/O module name	Slots	Notes
Step 2: Populate all Quad Port 10GbE SR I/O modules	Quad Port 10GbE SR	3, 4, 5, 6	Populate starting from the lowest available slot number.
Step 3: Populate all Quad Port 10 GBase-T I/O modules	Quad Port 10 GBase-T	3, 4, 5, 6	Populate starting from the lowest available slot number. With Quad Port 10 GBase-T in slot 1, max number of Quad Port 10 GBase-T I/O modules are limited to 4.
Step 4: Populate all Dual Port 16 Gbps Fibre Channel I/O modules	Dual Port 16 Gbps Fibre Channel	6, 5, 4, 3	Populate starting from the highest available slot number.

Internal system components

The following figure shows the layout of the CPUs and DIMMs inside the chassis. The front of the system is at the top of the figure.

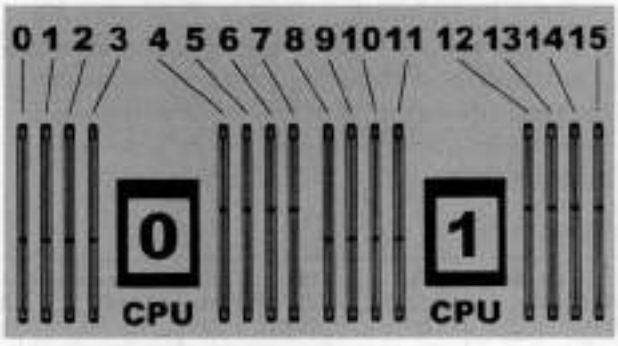


Figure 82. CPU and memory locations

DIMMs overview

Dual in-line memory modules (DIMM) come in various sizes, which must be configured in a certain way. This topic can help you select the correct configuration when servicing DIMMs.

The storage processor contains two Intel processors each with an integrated memory controller that supports four channels of memory. The storage processor allows two DIMM slots per channel, so the storage processor supports a total of 16 DIMM slots.

memory DIMM configuration

Table 76. memory DIMM configuration

Tier	Total Memory	Memory DIMM Configuration
DLH	192 GB	8 x 16 GB +8 x 8 GB
DLH Extended Retention/DD Cloud Tier	192 GB	8 x 16 GB +8 x 8 GB

HA is supported with all available memory configurations.

To ensure maximum memory performance, there are memory DIMM population rules for best memory loading and interleaving. Memory locations - CPU 0 and Memory locations - CPU 1 specify the DIMM location rules for various memory configurations:

Table 77. Memory locations - CPU 0

		Channel A		Channel B		Channel D		Channel C	
Tier	Total Memory	0	1	2	3	4	5	6	7
DLH (Base)	192 GB	16 GB	8 GB	16 GB	8 GB	8 GB	16 GB	8 GB	16 GB
DLH (Expanded)	192 GB	16 GB	8 GB	16 GB	8 GB	8 GB	16 GB	8 GB	16 GB

Table 78. Memory locations - CPU 1

		Channel A		Channel B		Channel D		Channel C	
Tier	Total Memory	8	9	10	11	12	13	14	15
DLH (Base)	192 GB	16 GB	8 GB	16 GB	8 GB	8 GB	16 GB	8 GB	16 GB
DLH (Expanded)	192 GB	16 GB	8 GB	16 GB	8 GB	8 GB	16 GB	8 GB	16 GB

DD6800 and ES30 shelf guidelines

The system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your system as listed in the following table below.
- Use the Installation and Setup Guide for your system to minimize the chance of a cabling mistake.
- A system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.
- DD6800 systems support ES30 SATA shelves after controller upgrades from older models.
- ES30 SATA shelves must be on their own chain.

Table 79. DD6800 and ES30 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	ES30 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB) [1]	Max RAW external capacity (TB) [2]
DD6800 w/ HA	192	2x4	SAS 30, 45, 60; SATA 15, 30, 45	7 [3]	4	144	180
DD6800 w/ Expanded Capacity [4]	192	2x4	SAS 30, 45, 60; SATA 15, 30, 45	7 [3]	4	288	360
DD6800 w/ Expanded Capacity w/ HA [4]	192	2x4	SAS 30, 45, 60	7 [3]	4	288	360
DD6800 w/ ER	192	2x4	SAS 30, 45, 60; SATA 15, 30, 45	7 [3]	4	576	720
DD6800 w/ DD Cloud Tier	192	2x4	SAS 30, 45, 60; SATA 15, 30, 45	7 [3]	4	288 (max), additional 96 SAS dedicated to DD Cloud Tier	360 (max), additional 120 SAS dedicated to DD Cloud Tier
DD6800 w/ HA and DD Cloud Tier [4]	192	2x4	SAS 30, 45, 60	7 [3]	4	288 (max), additional 96 SAS dedicated to DD Cloud Tier	360 (max), additional 120 SAS dedicated to DD Cloud Tier

1. This figure only counts drives that have user data in the shelves.

2. The raw capacity of an ES30 is 125% of the available capacity.

3. Recommended configurations start at four shelves per set and expand beyond that as required. For HA configurations, the ES15 counts as a shelf.

4. DDOS 6.x and later and ES15 SSD shelf configuration

Types of cabinets and power connections

The ES30 chassis is installed in two types of racks: 40U-C (existing racks) and the 40U-P (newer racks). The racks use one phase or 3-phase power connections.

3-Phase power connections for 40U-P (current racks)

Some environments use 3-phase power for 40U-P racks that are used for several systems. In those situations, it is desirable to balance the current draw across all three phases. The recommended 3-phase power cabling attempts to do that, but an optimal configuration depends on the specific installation.

Cabling shelves

NOTE:

- Before cabling the shelves, physically install all shelves in the racks. Refer to the rail kit installation instructions included with the ES30 shelf for rack mounting.
- The documentation refers to two SAS HBAs. If only one HBA is allowed in a system, then use another port as defined later for that specific system.
- On an HA system, add cables from the second node to open ports at the end of the sets. The ports on the second node must connect to the same sets as the corresponding ports on the first node.

Ports on the system's SAS HBA cards connect directly to a shelf controller's host port. For redundancy, you need to create dual paths by using a port on one SAS HBA card to connect to one shelf controller in each shelf set, and a port on another SAS HBA card to connect to another shelf controller in the same shelf set. With dual paths, if one SAS HBA card fails, the shelf is still operational. However, in the unlikely event any single shelf becomes completely disconnected from power or SAS cables and becomes disconnected from a previously operational shelf, the file system goes down and the shelf is not operational. This is considered a double failure.

There are two kinds of configurations: one shelf in a set or multiple shelves in a set.

DD6300, DD6800, and DD9300 shelf configurations

There are a few rules that must be followed when adding a mixture of DS60 and other shelf types to your system.

CAUTION: **If a system does not follow ALL of these rules it is not a legitimate configuration.**

Prerequisites:

- You cannot exceed the maximum amount of raw capacity displayed in the cabling table for each system.
- You cannot exceed the maximum number of shelves displayed in the cabling table for each system.
- There are no specific placement or cabling requirements for SSD shelves, or the metadata shelves for Cloud Tier configurations. These shelves can be installed and cabled the same way as standard ES30 shelves.

Table 80. Minimum and maximum configurations

System	Appliance	Minimum appliance shelf count*	Max appliance shelf count
	48 TB usable	0	1
w/ Expansion	144 TB usable	1	5
	144 TB usable	2	28
w/ Expansion	288 TB usable	2	28
w/ High Availability (HA)	288 TB usable	2	28
w/ Extended Retention (ER)	576 TB usable	2	28
w/ Cloud Tier	288 TB usable (96 TB for Cloud Tier)	2	28
w/ HA and Cloud Tier	288 TB usable (96 TB for Cloud Tier)	2	28
	384 TB usable	3	28
w/ Expansion	720 TB usable	3	28

Table 80. Minimum and maximum configurations (continued)

System	Appliance	Minimum appliance shelf count*	Max appliance shelf count
w/ HA	720 TB usable	3	28
w/ ER	1440 TB usable	7	28
w/ Cloud Tier	720 TB usable (192 TB for Cloud Tier)	7	28
w/ HA and Cloud Tier	720 TB usable (192 TB for Cloud Tier)	7	28

* The minimum appliance shelf count does not include shelves for Cloud Tier.

DD6800 and DS60 shelf guidelines

The system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your system as listed in the following table.
- For redundancy, the two connections from a system to a set of shelves must use ports on different SAS I/O modules.
- Use the Installation and Setup Guide for your system to minimize the chance of a cabling mistake.
- A system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.
- ES30 SATA shelves must be on their own chain.
- If ES30 SAS shelves are on the same chain as a DS60, the maximum number of shelves on that chain is 5.

Table 81. DD6800 and DS60 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	DS60 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB)[1]	Max RAW external capacity (TB)
DD6800 [2, 3, 4]	192	2x4	SAS 45, 60	1	1	144	180
DD6800 w/ Expanded Capacity [2, 3]	192	2x4	SAS 45, 60	1	2	288	360
DD6800 w/ Expanded Capacity and w/ HA [2, 3]	192	2x4	SAS 45, 60	1	2	288	360
DD6800 w/ Expanded Capacity and w/ ER [2, 3]	192	2x4	SAS 45, 60	2	4	576	720
DD6800 w/ Expanded Capacity and w/ Cloud Tier [3, 5]	192	2x4	SAS 45, 60	2	4	288 + 96 for DD Cloud Tier	360 + 120 for DD Cloud Tier
DD6800 w/ Expanded Capacity and w/ Cloud Tier and HA [3, 5]	192	2x4	SAS 45, 60	2	4	288 + 96 for DD Cloud Tier	360 + 120 for DD Cloud Tier

NOTE: An entry of 45 corresponds to DS60-3 models and an entry of 60 corresponds to DS60-4 models.

1. This column only counts drives that have user data in the shelves. For example, a DS60 4-240 has 192TB.

2. With DD OS 6.x (or greater) & SSD.

3. Only available with DD OS 6.x and greater.

4.DD6800 base configuration has the same configuration as the DD6800 Expanded. Maximum capacity is limited by capacity license.

5. With Cloud Tier Storage.

shelf configurations

There are a few rules that must be followed when adding a mixture of DS60 and other shelf types to your system.

CAUTION: **If a system does not follow all these rules, it is not a legitimate configuration.**

Prerequisites:

- You cannot exceed the maximum amount of raw capacity displayed in cabling table for each system.
- You cannot exceed the maximum number of shelves displayed in cabling table for each system.
- You cannot connect more than three DS60 shelves in a single set.

Table 82. Minimum configurations

System	Appliance maximum	Minimum appliance DS60 shelf count
	144 TB	0
	144 TB	2
w/ High Availability (HA)	288 TB	2 (plus 1 FS15 for SSD cache)
w/ Extended Retention (ER)	576 TB	2
w/ Cloud Tier	384 TB (96 TB for Cloud Tier)	2 (plus 2 ES30s for Cloud Tier)
w/ HA and Cloud Tier	384 TB (96 TB for Cloud Tier)	2 (plus 1 FS15 for SSD cache, and 2 ES30s for Cloud Tier)
	384 TB	3
w/ HA	720 TB	3 (plus 1 FS15 for SSD cache)
w/ ER	1440 TB	3
w/ Cloud Tier	912 TB (192 TB for Cloud Tier)	3 (plus 4 ES30s or 1 DS60 for Cloud Tier)
w/ HA and Cloud Tier	912 TB (192 TB for Cloud Tier)	4 (plus 1 FS15 for SSD cache, and 4 ES30s or 1 DS60 for Cloud Tier)

1. DS60 will only be partially filled.

- A Cloud Tier system shares the ERSO cabling configuration; however, Cloud Tier has a lower maximum.
- It is recommended that the shelf with the greater number of drives should always be placed in the bottom position.
- only supports one DS60.
- only has one SAS SLIC and all DS60 connections are made to that single SAS SLIC.
- only has one SAS SLIC and all DS60 connections are made to that single SAS SLIC.

8

DD6900

This chapter contains the following topics:

Topics:

- DD6900 system features
- DD6900 system specifications
- DD6900 storage capacity and configurations
- DD6900 front panel
- DD6900 SSD usage and configurations
- Rear panel
- PCIe HBAs
- DD6900 DIMM configurations
- DD6900, DD9400, and DD9900 storage shelves configurations and capacities

DD6900 system features

Table 83. DD6900 system features

Feature		Single Node	HA
Processor		2 x Intel Xeon 4208, 8C, 2.10GHz, 85W	
Kernel		4.4	
Memory Configurations	Total	288 GB	
	DIMMs	12 x 8 GB + 12 x 16 GB	
HDD Drive Size		4TB (3 TB supported after controller upgrade)	
Supported Capacity	Active Tier	24 <-> 288 TBu	
	Cloud Tier	576 TBu	
Disk Groups	Active Tier	1 <-> 6 (4 TB), 1 <-> 8 (3 TB)	
	Cloud Tier (4 TB)	2	
SSDs for DD OS in 2.5' bay in the head		4, 0.96 TB, 1 WPD	
Stream Count		400 Wr, 110 Rd	
Cache SSDs	1.2%	2 (Internal) 1.92 TB	2 (External FS25) 3.84 TB
Cache SSD shelf	FS25	0	1
HA Private Interconnect		N/A	(2) 10G Base-T ports (NDC)
16 GB NVRAM		1	
HW Accelerator	100 Quick Assist Technology (QAT) 8970	1	
Internal SAS	HBA330 12 Gbps SAS controller	1	
External SAS	PMC Quad Port 12 Gbps SAS	2 default, 3 supported	
SAS String Depth (max)	ES30/ES40	7	

Table 83. DD6900 system features (continued)

Feature		Single Node	HA
	DS60	2	
Host Interface HBAs	2-port QL41000 25 GbE-SFP28	4 maximum	
	4-port QL41164 10 GbE-SFP+	3 maximum	
	4-port QL41164 10GBASE-T	4 maximum	
	4-port QLE2694 16 Gb FC	3 maximum	
Network Daughter Card option (system will have one of the two options)	4-port QL41000 10 GbE-SP+ FasLinQ	1	
	4-port QL41164 10GBASE-T	1	

DD6900 system specifications

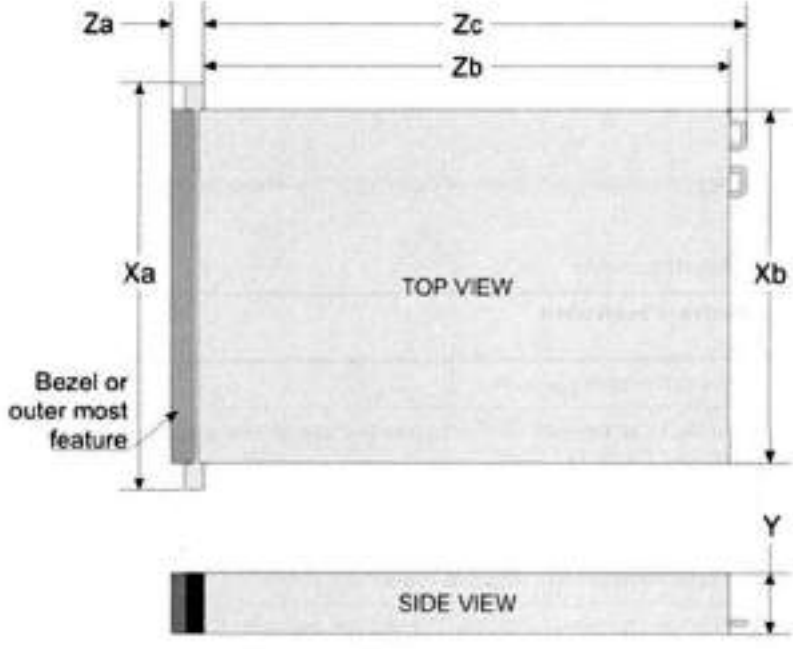


Figure 83. System dimensions

Table 84. DD6900 system specifications

Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb	Zc
482.0 mm (18.98 inches)	434.0 mm (17.09 inches)	86.8 mm (3.42 inches)	35.84 mm (1.41 inches)	22.0 mm (0.87 inches)	678.8 mm (26.72 inches)	715.5 mm (28.17 inches)

A DD6900 system weighs up to 63.05 lbs (28.6 kg).

Table 85. System operating environment

Operating Temperature	50° to 95° F (10° to 35° C), derate 1.1° C per 1000 feet, above 7500 feet up to 10,000 feet (32.25° C at 10,000
Operating Humidity	20% to 80%, non-condensing
Non-operating Temperature	-40° to +149° F (-40° to +65° C)

Table 85. System operating environment (continued)

Operating Acoustic Noise	L_{wad} sound power, 7.5 Bels

DD6900 storage capacity and configurations

The following table provides storage capacity and configuration information for the DD6900 system:

Table 86. DD6900 storage capacity and configurations

Tier	CPU-SP SKU	Memory	Front 2.5" SSDs	Max. Useable Capacity	Cloud Tier Metadata
DD6900	8 core, 85 W 4208	288 GB (12 x 16 GB) + (12 x 8 GB)	1 (1.2%)	288 TB	N/A
DD6900 with DD Cloud Tier[1]	8 core, 85 W 4208	288 GB (12 x 16 GB) + (12 x 8 GB)	1 (1.2%)	576 TB	120 TB raw/96 TB usable

[1] DD Cloud Tier can be added to a DD6900 and is enabled by a license and disk packs for the DD Cloud Tier metadata.

The Memory column lists the total memory that is required and the number and type of the DIMMs used. All memory DIMMs are DDR4 RDIMMs at the highest supported speed of 2400MT/s.

High Availability

DD6900 supports Active-Passive High Availability (A-P HA or just A-P). The following table summarizes the hardware changes to support A-P HA:

Table 87. HA configuration requirements

Hardware Change to support HA	Active-Passive HA
Additional memory	No extra memory required.
HA private interconnect	Cluster interconnect : A-P requires the use of two ports from the on-board quad-port 10 GbE Network Daughter Card.
NVRAM	A-P requires a single 16 GB NVRAM card (same as non-HA).
SAS Connectivity	Both nodes of an A-P HA pair require redundant SAS connectivity to the storage array. (Note: a single node system also has redundant connectivity to the storage array.)
SSD Requirements	SSDs are contained within FS25 and are available from both nodes.

HA Network Interconnect

The HA Network Interconnect, required for HA configurations, is a dedicated 10 GbE connection between the two nodes of an HA pair. The interconnect is used to write data (and metadata) from the active node's NVRAM to the passive node's NVRAM.

Two 10GbE links are used to meet the bandwidth requirements for the private interconnect. Traffic across the private interconnect has roughly the same bandwidth as is written to the NVRAM card. The dual 10-GbE links can move about 2 GB/s in each direction.

HA SAS Interconnect

HA configurations require that the SSDs' cache drives be shared between both nodes and have redundant SAS connections to all shelves.

DD6900 front panel

Figure 84. DD6900 front panel

Table 88. Front panel features

Item	Ports, panels, and slots	Description
1	Left control panel	Contains system health and system ID, status LED, and optional iDRAC Quick Sync 2 (wireless).
2	Drive slots	Enable you to install drives that are supported on your system.
3	Right control panel	Contains the power button, VGA port, iDRAC Direct micro USB port, and two USB 2.0 ports.
4	Information tag	The Information tag is a slide-out label panel that contains system information such as Service Tag, NIC, MAC address, and so on. If you have opted for the secure default access to iDRAC, the Information tag also contains the iDRAC secure default password.

Table 89. Front LEDs

Name	Color	Purpose
Control Panel Status LED	Blue/Amber	Status: • Healthy: Solid Blue • Fault: Blink Amber • Sys ID: Blink Blue
System Power Button/LED	Green	Indication that the system has power.
Drive activity LEDs	Green	Lit green when the drive is powered. Blinks during drive activity.
Drive service LEDs	Green	Lit solid amber when a disk drive needs service.

Front LEDs

Figure 85. Front left control panel status LEDs

NOTE: The indicators display solid amber if any error occurs.

Table 90. System health and system ID indicator codes

System health and ID indicator code	
Solid blue	Indicates that the system is turned on, system is healthy, and system ID mode is not active. Press the system health and system ID button to switch to system ID mode.
Blinking blue	Indicates that the system ID mode is active. Press the system health and system ID button to switch to system health mode.
Solid amber	Indicates that the system is in fail-safe mode.
Blinking amber	Indicates that the system is experiencing a fault. Check the System event log or the LCD panel, if available on the bezel, for specific error messages.

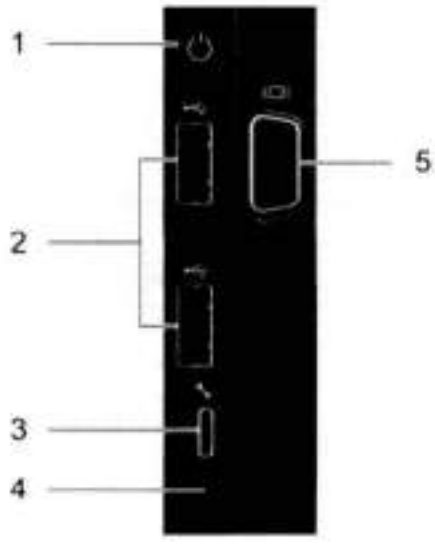


Figure 86. Front right control panel power button LEDs

Table 91. Right control panel features

Item	Indicator, button, or connector	Description
1	Power button	Indicates if the system is turned on or off. Press the power button to manually turn on or off the system. **NOTE:** Press the power button to gracefully shut down an ACPI-compliant operating system.

Table 91. Right control panel features (continued)

Item	Indicator, button, or connector	Description
2	USB port (2)	The USB ports are 4-pin, 2.0-compliant. These ports enable you to connect USB devices to the system.
3	iDRAC Direct port	The iDRAC Direct port is micro USB 2.0-compliant. This port enables you to access the iDRAC Direct features.
4	iDRAC Direct LED	The iDRAC Direct LED indicator lights up to indicate that the iDRAC Direct port is connected.
5	VGA port	Enables you to connect a display device to the system.

Table 92. iDRAC Direct LED indicator codes

iDRAC Direct LED indicator code	Condition
Solid green for two seconds	Indicates that the laptop or tablet is connected.
Flashing green (on for two seconds and off for two seconds)	Indicates that the laptop or tablet that is connected is recognized.
Turns of	Indicates that the laptop or tablet is unplugged.

Figure 87. Drive LEDs

The front contains 25 2.5" disk drive slots that can be populated with SSDs. Each SSD is housed in a drive carrier that contains two LEDs at the bottom of the carrier. The carrier's left blue LED is lit whenever an SSD is present in the slot, and it blinks when I/O activity is occurring on the disk. The right amber LED is usually off and lights amber to indicate that the disk is faulted and must be serviced.

DD6900 SSD usage and configurations

DD6900 system uses an 8 x 2.5" drive slot midplane. In addition to the four 0.96TB SSD DD OS drives, two 1.92TB SSDs are needed for the metadata cache implementation for single node systems. For DD6900 HA systems, two 3.84 TB SSDs cache drives are used in the external FS25 shelf.

SSD configurations

The SSD slots on the front of the enclosure are shown below. The system come from the factory with SSDs populated in the enclosure.

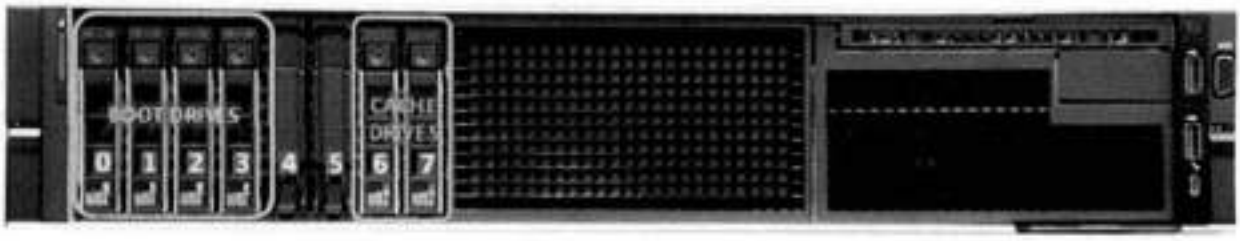


Figure 88. DD6900 SSD slot assignment

DD6900 supports 12% SSD options out of factory configurations. Based on 3.84 TB SSD capacity, the required number of SSDs for each DD6900 configuration is provided in the following table.

Table 93. DD6900 SSD configurations

Configuration	Single node	HA
Cache SSDs	2 (internal) 1.92 TB	2 (External FS25) 3.84 TB

The cache SSDs are installed right to left starting from slot 7 down.

SSD boot drives

Other SAS SSDs are used to boot the DD OS operating system. Boot disks and external disk shelves are used to log system information. Boot disks are installed from the other end of the front 2.5" disk slots to physically differentiate the cache SSDs.

Table 94. SSD boot drives

# of boot disks	Installed in slots
Four 0.96TB SSDs	0,1,2,3

Rear panel

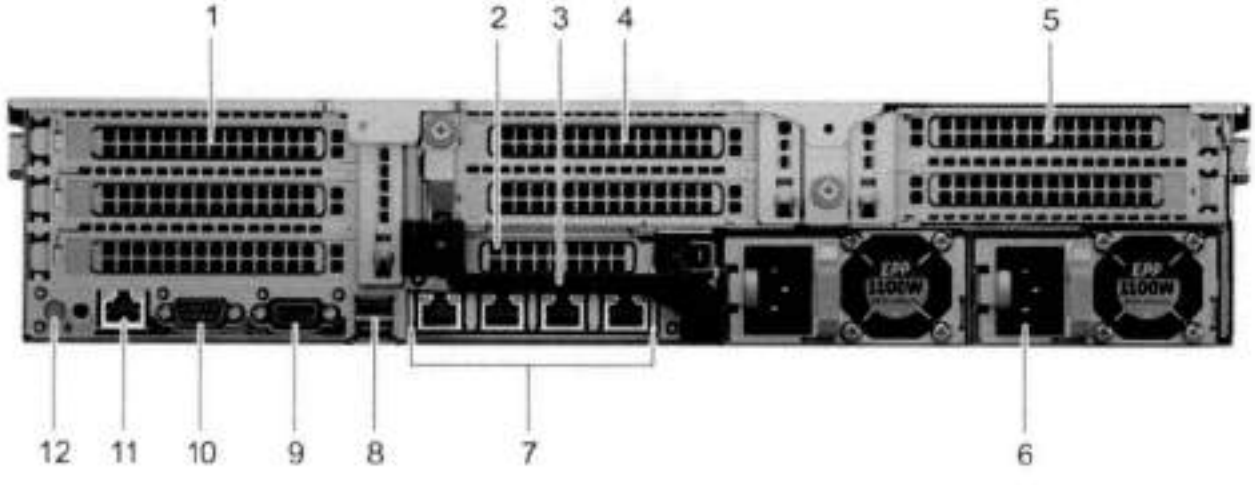


Figure 89. System rear panel

Item	Panels, ports, and slots	Description
1	Full-height PCIe expansion card slot (3)	The PCIe expansion card slot (riser 1) connects up to three full-height PCIe expansion cards to the system.

Item	Panels, ports, and slots	Description
2	Half-height PCIe expansion card slot	The PCIe expansion card slot (riser 2) connects one half-height PCIe expansion cards to the system.
3	Rear handle	The rear handle can be removed to enable any external cabling of PCIe cards that are installed in the PCIe expansion card slot 6.
4	Full-height PCIe expansion card slot (2)	The PCIe expansion card slot (riser 2) connects up to two full-height PCIe expansion cards to the system.
5	Full-height PCIe expansion card slot (2)	The PCIe expansion card slot (riser 3) connects up to two full-height PCIe expansion cards to the system.
6	Power supply unit (2)	Supports two AC power supply units (PSUs)
7	NIC ports	The NIC ports that are integrated on the network daughter card (NDC) provide network connectivity.
8	USB port (2)	The USB ports are 9-pin and 3.0-compliant. These ports enable you to connect USB devices to the system.
9	VGA port	Enables you to connect a display device to the system.
10	Serial port	Enables you to connect a serial device to the system.
11	iDRAC9 dedicated port	Enables you to remotely access iDRAC.
12	System identification button	The System Identification (ID) button is available on the front and back of the systems. Press the button to identify a system in a rack by turning on the system ID button. You can also use the system ID button to reset iDRAC and to access BIOS using the step through mode.

Rear LEDs

Figure 90. Onboard ID and iDRAC LEDs

1. iDRAC management port:
   a. The green link LED on the left is lit whenever there is link at 1000BaseT and 100BaseT speeds. The link LED is off when the link speed is 10BaseT or there is no link.
   b. The green link LED on the right blinks whenever there is traffic on the port.
2. System identification LED: This blue LED can be turned on by software to visually identify the system.

PSU FRU LEDs

There are two power supplies, one in the upper left of the rear chassis and one on the bottom right. Each power supply has three LEDs: AC good, DC good, and Service. The top PSU is "right-side up" and the bottom PSU is "upside down."

Table 95. PSU FRU LEDs

Name	Color	Definition
AC Good	Green	AC input is as expected.
DC Good	Green	DC output is as expected.
Service	Amber	PSU has a fault condition and a must be replaced.

PCIe HBAs

A slot in the chassis that does not contain an HBA must have a filler panel installed in the empty slots. This is required for EMI compliance.

This system supports nine I/O modules slots, seven of which are 8-lane PCIe Gen3, and two are 16-lane PCIe Gen3. Several networking, NVRAM, SAS, and Fibre Channel I/O modules are supported.

Slot assignment

The following table lists the DD6900 configuration slot assignments:

Table 96. DD6900 slot assignments

Description	Slot
QLogic, 41164 4 Port, 10GbE SFP+ PCIe, Full Height	5, 8, 1
QLogic, 41164 4 Port, 10GBASE-T PCIe, Full Height	5, 8, 1
QLogic, 41164 4 Port, 10GBASE-T PCIe, Low Profile	6
QLogic, 41262 2 Port, 25Gb SFP28 PCIe, Full Height	5, 8, 1
QLogic, 41262 2 Port, 25Gb SFP28 PCIe, Low Profile	6
HBA330 SAS Controller, 12Gbps Mini card	mini/mono
QAT,INTEL,8970,FH, Avnet p/n 1QA89701G1P5	4
PM8072,SAS12,4P,FH, MicroSemi 2295200-R	3, 7, 5
FC16,QLE2694-DEL-BK,TRG,QP,FH	5, 8, 1
16GB NVRAM,FH	2

Host Interface (x16) is 2-port 100 Gb QSFP+ Ethernet.

Host Interface (x8) are:

- 2-port 25 Gb SFP28 Ethernet
- 4-port 10 Gb SFP+ Ethernet
- 4-port 10GBaseT Ethernet
- 4-port 16 Gb Fibre Channel

External SAS is 4-port 12 Gb SAS card and is required for external storage for HA and Single Node configurations.

NVRAM is the 16GB NVRAM.

Internal SAS Mezzanine is 2-port 12 Gb Mini-SAS HD SAS controller mezzanine.

Host Network Interface Mezzanine is either:

- 4-port 10GBaseSR SFP+ Ethernet mezzanine
- 4-port 10GBaseT RJ45 Ethernet mezzanine

I/O population rules

The following figures show the I/O module slot numbers.

The slot labeled N is the network daughter card, which contains ports ethMa, ethMb, ethMc, and ethMd.

The physical interface name format for the other I/O module slots is `ethXy`, where X is the slot number and y is an alphanumeric character. For example, eth0a.

For most horizontal I/O module NIC interfaces, the port numbering goes from left to right, with ethXa on the left. The horizontal I/O module slots on the left-in slots 1-3 are inverted. The port numbering on these I/O modules in these slots goes from right to left, with ethXa on the right.

The management port ethMa is the first port set up by the Configuration Wizard. It is marked with a red rectangle in the figure below.

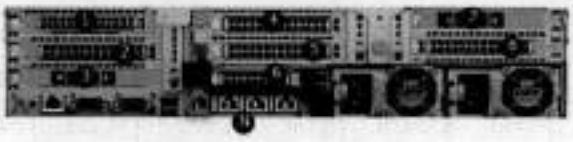


Figure 91. Slot numbering

The general population rules can be summarized as:

1. Populate a given I/O in the available slots listed.
2. Select the first available slot in the group.
3. Follow the steps for each I/O in the order specified.
4. Slots 4 and 8 should be reserved for x16 cards unless there are no available x8 slots.

NOTE: Installing HBAs requires opening the system and installing the HBA into the riser.

Riser#	Slots (from top to bottom)
1	1, 2, 3
2	4, 5, 6, N
3	7, 8

Gen3 PCIe

Slots support Gen3 PCIe.

I/O module servicing

All I/O modules are user serviceable and may be replaced when the system is powered off. On-line service of I/O modules is not support. A module that is hot-inserted into the system will remain powered off and will not be powered on until the next reboot of the system. A module that is hot-removed causes an operating system to immediately reboot.

DD6900 DIMM configurations

The SP Module contains two Intel SP processors each with an integrated memory controller that supports six channels of DDR4 memory. The CPU enables two DIMM slots per channel, so the SP Module supports 24 DIMM slots.

Each DDR4 DIMM is connected to the system board through an industry standard 288-pin DDR4 DIMM connector. This system uses registered DIMMs with Dell EMC ControlCenter at 72 bits wide (64-bits data + 8-bits Dell EMC ControlCenter) up to a maximum of 2400MT/s speed.

Table 97. Memory configurations

Tier	Total Memory	Memory DIMM Configuration
DD6900 Active Tier	288 GB	12 x 8 GB + 12 x 16 GB
DD6900 Cloud Tier	288 GB	12 x 8 GB + 12 x 16 GB

Memory locations

To ensure maximum memory performance, there are memory DIMM population rules so that the memory loading and interleaving are optimal. The following table specifies the DIMM location rules. Each DIMM location contains either a 8GB DIMM or a 16GB DIMM.

Table 98. DD6900 DIMM configuration CPU 1

Total (GB)	Channel C		Channel B		Channel A		Channel D		Channel E		Channel F	
	A6	A12	A5	A11	A4	A10	A7	A1	A8	A2	A9	A3
144	16 GB	8 GB	16 GB	8 GB	16 GB	8 GB	8 GB	16 GB	8 GB	16 GB	8 GB	16 GB

Table 99. DD6900 DIMM configuration CPU 2

Total (GB)	Channel C		Channel B		Channel A		Channel D		Channel E		Channel F	
	B6	B12	B5	B11	B4	B10	B7	B1	B8	B2	B9	B3
144	16 GB	8 GB	16 GB	8 GB	16 GB	8 GB	8 GB	16 GB	8 GB	16 GB	8 GB	16 GB

DD6900, DD9400, and DD9900 storage shelves configurations and capacities

DD6900, DD9400, and DD9900 do not store data on internal disk drives and rely on external disk array shelves to provide storage. DS60 disk shelves and ES40 shelves are connected to systems using 12 Gb Mini-SAS HD ports, which are implemented on the SAS HBAs.

The systems also support external metadata storage (cache) shelf FS25. External cache shelf only hosts DD OS depended metadata for performance acceleration.

The ES40 SAS shelf contains 15 drives, which includes 12 drives of usable storage, two parity drives, and one hot spare.

The DS60 shelf contains 60 drives. Drives are configured in four groups of 15 drives. Each group contains two parity drives and one hot spare, so each group provides 12 drives of usable storage. A fully configured DS60 shelf provides 48 drives of usable storage.

Table 100. Shelves shipped from factory, in rack

DD6900	DD9400	DD9900
4 TB ES40	8 TB DS60	8 TB DS60

Table 101. Shelves shipped from factory, boxed

DD6900	DD9400	DD9900
4 TB ES40	8 TB ES40	8 TB ES40
4 TB DS60	8 TB DS60	8 TB DS60

Table 102. Additional shelves supported

DD6900	DD9400	DD9900
4 TB SAS ES30/DS60	4 TB SAS ES30/DS60	4 TB SAS ES30/DS60

Table 102. Additional shelves supported (continued)

DD6900	DD9400	DD9900
3 TB SAS ES30/DS60	3 TB SAS ES30/DS60	3 TB SAS ES30/DS60

NOTE: 3 TB shelves are only support on controller upgrades and not on fresh installs.

Table 103. Shelf usable capacities

Hard drive size (TB)	Shelf	Useable TB
4	ES40	48
4	DS60	192
8	DS60	384

The following table lists the maximum number of shelves per chain:

Table 104. Supported shelf count per chain

Shelf type	Max # from factory	Max # per chain
SAS ES30/ES40	4	7
DS60	2	3
DS60 + ES30/ES40	n/a	5
F25	1	1

The connector type for ES30 is Mini-SAS. Special cables may be necessary when combining ES30 and ES40 shelves on the same chain (enabled but not recommended).

DD9400 and DD9900 system capacities are optimized for use with DS60 shelves containing 8 TB drives. DS60 shelves can be populated with one to four packs of fifteen 8 TB, or 4 TB drives. Different 4 TB and 8 TB capacity disk packs may be mixed within a single DS60 shelf. ES40 SAS shelves and DS60 shelves of mixed capacities may be attached so long as the maximum storage capacity of the system is not exceeded.

9

DD7200

This chapter contains the following topics:

Topics:

- DD7200 system features
- DD7200 system specifications
- DD7200 storage capacity
- Front Panel
- Back Panel
- I/O modules and slot assignments
- Internal system components
- DD7200 and ES30 shelf guidelines
- DD7200 and DS60 shelf guidelines

DD7200 system features

The table summarizes the DD7200 system features.

Table 105. DD7200 system features

Feature		DD7200 (Base configuration)	DD7200 (Expanded configuration)
Rack height		4U, supported in four-post racks only	4U, supported in four-post racks only
Rack mounting		Rack mount kit included with each system. Adjustable between 24 - 36 in. (60.9 - 76.2 cm).	Rack mount kit included with each system. Adjustable between 24 - 36 in. (60.9 - 76.2 cm).
Power		1 +1 redundant, hot-swappable power units	1 +1 redundant, hot-swappable power units
Processor		Two 8-core processors	Two 8-core processors
NVRAM		One 4-GB NVRAM module (and companion BBU) for data integrity during a power outage	One 4-GB NVRAM module (and companion BBU) for data integrity during a power outage
Fans		Hot-swappable, redundant, 5	Hot-swappable, redundant, 5
Memory		8 x 16 GB DIMM (128 GB)	16 x 16 GB DIMM (256 GB)
Internal drives		SSD drives, 3 x 200 GB (base 10)	SSD drives, 3 x 200 GB (base 10)
I/O module slots		Nine replaceable I/O module (Fibre Channel, Ethernet, and SAS) slots, one BBU, one NVRAM, and one Management module slot. See Management module and interfaces and I/O modules and slot assignments.	Nine replaceable I/O module (Fibre Channel, Ethernet, and SAS) slots, one BBU, one NVRAM, and one Management module slot. See Management module and interfaces and I/O modules and slot assignments.
Supported capacity	Non-extended retention	12 x 2-TB or 8 x 3-TB shelves adding up to 285 TB of usable external capacity.	8 x 2-TB or 12 x 3-TB shelves adding up to 428 TB of usable external capacity.
	DD Cloud Tier	N/A	428 TB of Active Tier capacity, and 856 TB of Cloud Tier capacity. 4 x 4 TB shelves are required to store DD Cloud Tier metadata.
	DD Extended Retention	N/A	56 shelves adding up to a maximum of 856 GB of usable external capacity.

DD7200 system specifications

Table 106. DD7200 system specifications

Model	Watts	BTU/hr	Power	Weight	Width	Depth	Height
DD7200	800	2730	800	80 lb / 36.3 kg	17.5 in (44.5 cm)	33 in (84 cm)	7 in (17.8 cm)

Table 107. System operating environment

Operating Temperature	50° to 95° F (10° to 35° C), derate 1.1° C per 1000 feet, above 7500 feet up to 10,000 feet
Operating Humidity	20% to 80%, non-condensing
Non-operating Temperature	-40° to +149° F (-40° to +65° C)
Operating Acoustic Noise	Sound power, LWAd: 7.52 bels. Sound pressure, LpAm: 56.4 dB. (Declared noise emission per ISO 9296.)

DD7200 storage capacity

The table lists the capacities of the systems. Data Domain system internal indexes and other product components use variable amounts of storage, depending on the type of data and the sizes of files. If you send different datasets to otherwise identical systems, one system may, over time, have room for more or less actual backup data than another.

Table 108. DD7200 storage capacity

System/ Installed Memory	Internal Disks (SATA SSDs)	Data Storage Space	External Storage[3]
DD7200 (2 SAS I/O modules) 128 GB	2.5 in. 3 @ 200 GB No User Data	285 TB	Up to a maximum of 12 x 2-TB or 8 x 3-TB shelves.
DD7200 (2 SAS I/O modules) 256 GB	2.5 in. 3 @ 200 GB No User Data	428 TB	Up to a maximum of 18 x 2-TB or 12 x 3-TB shelves.
DD7200 with DD Cloud Tier[1] (4 SAS I/O modules) 256 GB	2.5 in. 3 @ 200 GB No User Data	• 428 TB (Active Tier) • 192 TB (DD Cloud Tier metadata) • 856 TB (DD Cloud Tier)	Up to a maximum of 18 x 2-TB or 12 x 3-TB shelves. 4x4-TB shelves for DD Cloud Tier metadata.
DD7200 with Extended Retention software[1] (4 SAS I/O modules) 256 GB	2.5 in. 3 @ 200 GB No User Data	856 TB	Up to a maximum of 36 x 2-TB or 24 x 3-TB shelves.

[1]Data Domain DD7200 controller with DD Extended Retention software.

[2] Data Domain DD7200 controller with DD Cloud Tier.

[3] The capacity differs depending on the size of the external storage shelves used. This data based on ES30 shelves.

Front Panel

The photo shows the hardware features and interfaces on the front of the system.

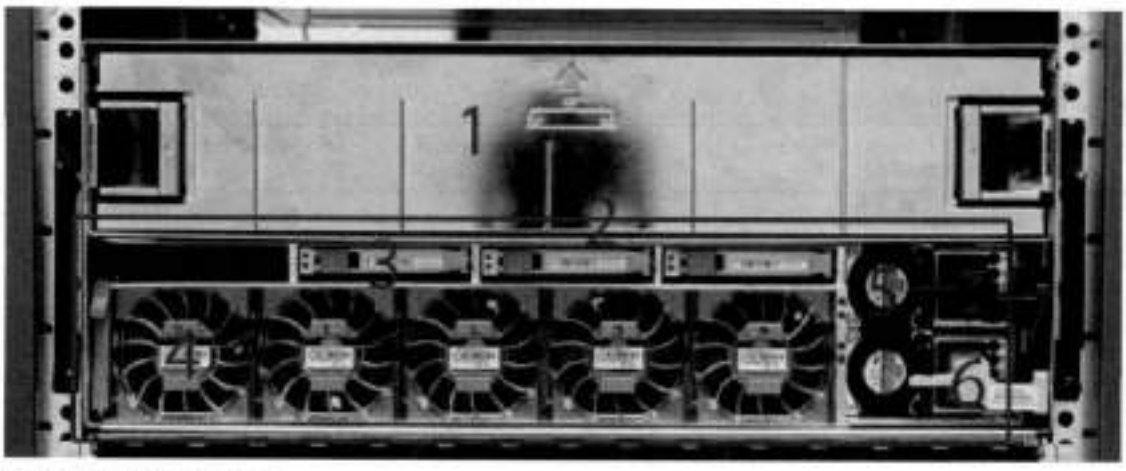


Figure 92. Front panel components

(1)	Filler panel
(2)	The red box indicates the system processor (SP) module
(3)	SSD drive #1
(4)	Fan #0
(5)	Power supply #0
(6)	AC power disconnect plug
(7)	AC power extender module

Power supply units

A system has two power supply units, numbered A and B from the bottom up. Each power supply has its own integral cooling fan. Each power unit has three LEDs (see System LED legend label) that indicates the following states:

- AC LED: Glows green when AC input is good
- DC LED: Glows green when DC output is good
- Symbol "!": Glows solid or blinking amber for fault or attention

The AC power plugs are located to the right of each power supply. These plugs are pulled to disconnect AC power to each power supply.

AC power extender module

AC power entry is connected at the rear of the system. The AC power extender module provides power to the two power supplies on the front of the system. AC Power plugs are located in the front. The module is adjacent to the SP module and can be removed and replaced.

Cooling Fans

A system contains five hot-swappable cooling fans in a 4+1 redundant configuration. The fans provide cooling for the processors, DIMMs, IO modules, and the management module. Each fan has a fault LED which causes the fan housing to glow amber. A system can run with one fan faulted or removed.

Solid-state drives

A system contains three hot-swappable 2.5" solid-state drive (SSD) bays that are located in the front and on top of the fan modules. There are four drive bays, with the left-most bay containing a blank. The next drive to the right of the blank is SSD #1, the next is #2, and the right-most bay contains SSD #3. No user backup data is kept on the SSDs.

Each drive has a blue colored power LED and an amber fault LED.

Front LED Indicators

The photo below indicates the location of the four system LEDs.

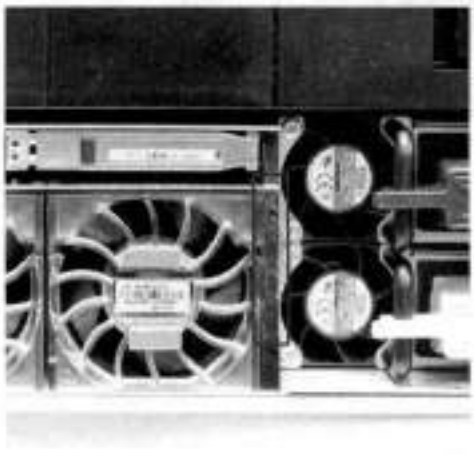


Figure 93. System LEDs

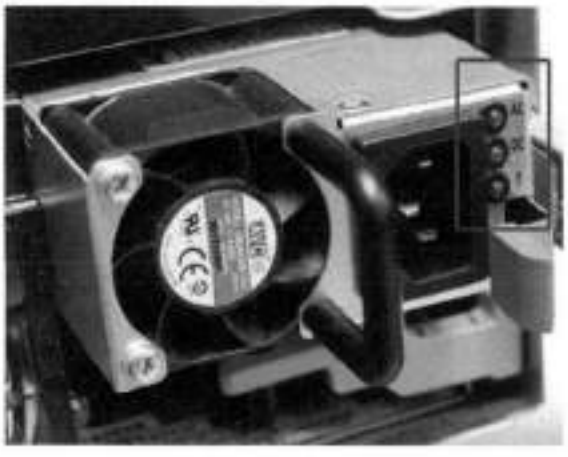
The next photo shows the location of the system LED legend label. Power supply LEDs shows the power supply LEDs. Other front LEDs are shown in Fan and SSD LEDs. LED states are described in LED status indicators.

Figure 94. System LED legend label

The power supply LEDs include:

- AC LED on top
- DC LED in the middle
- Failure LED on the bottom

Figure 95. Power supply LEDs



Each SSD has two LEDs as shown in the following figure. The lower left corner of the housing around each fan acts as an LED, glowing amber when the fan has failed.

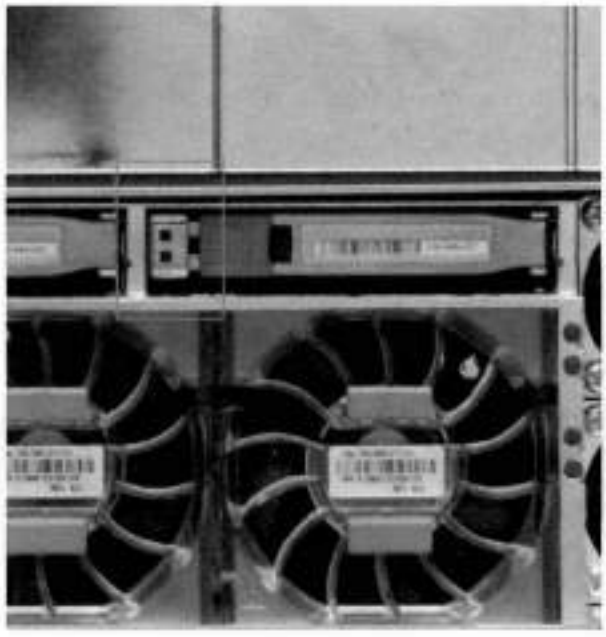


Figure 96. Fan and SSD LEDs

Table 109. LED status indicators

Part	Description or Location	State
System	Dot within a circle (top LED)	Blue indicates power on and normal operation.
System, SP fault	Exclamation point within a triangle	Dark indicates normal operation. Amber indicates failure.
System, chassis fault	Exclamation point within a triangle with a light below	Dark indicates normal operation. Yellow indicates a fault condition.
System	Marked out hand within a black square (bottom LED)	White warms not to remove the unit.
Power supply	AC LED	Steady green indicates normal AC power.
Power supply	DC LED	Steady green indicates normal DC power.
Power supply	Failure LED	Solid amber indicates a failed power supply.
SSD	Top LED	Solid blue, disk ready, blinks while busy.
SSD	Bottom LED	Dark indicates healthy. Solid amber indicates disk fail.
Fan	Fan housing	The fan housing glows an amber color during fan failure.

Back Panel

The photo shows the hardware features and interfaces on the back of the system.

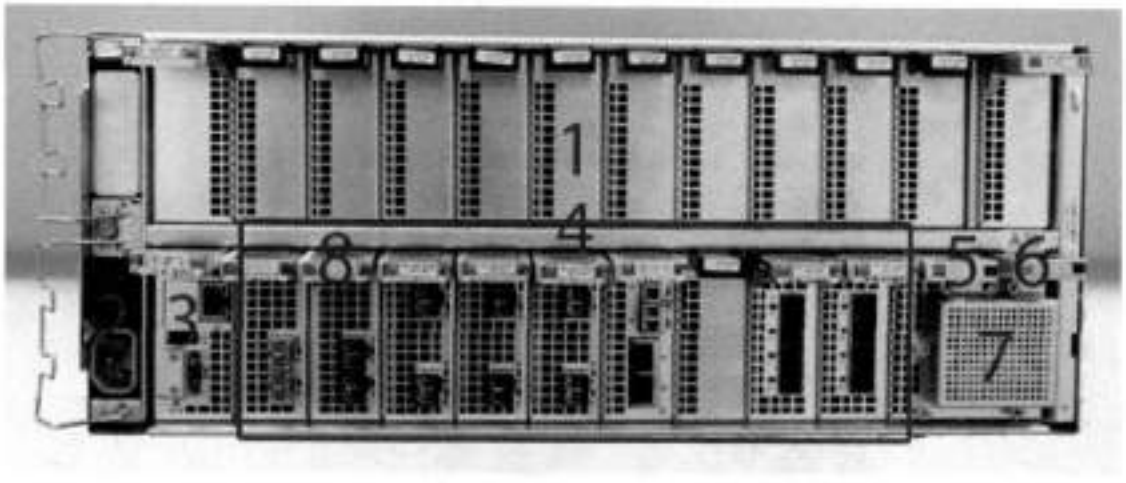


Figure 97. Features on rear of chassis

1. Upper level contains all blanks
2. AC power extender module
3. Management module (slot Mgmt A)
4. Red box indicating I/O modules (slots 0-8)
5. Battery backup (BBU in slot 9)
6. NVRAM module (slot 10)
7. Cage covering the BBU and NVRAM combination module
8. I/O LED at the end of each I/O module handle
9. Location of serial number label/tag

NOTE: For modules containing multiple ports, the bottom port is numbered as zero (0) with numbers increasing going upward.

I/O module LEDs

Each I/O module ejector handle contains a bi-colored LED. Green indicates normal function, while an amber color indicates a fault condition.

Management module and interfaces

The management module is on the left-most side when facing the back of the system, in slot Mgmt A. The process to remove and add a management module is the same as the I/O modules, however, the management module can only be accommodated in Mgmt A slot.

The management module contains one external LAN connection for management access to the SP module. One micro DB-9 connector is included to provide the console. A USB port is provided for use during service of the system to allow booting from a USB flash device.

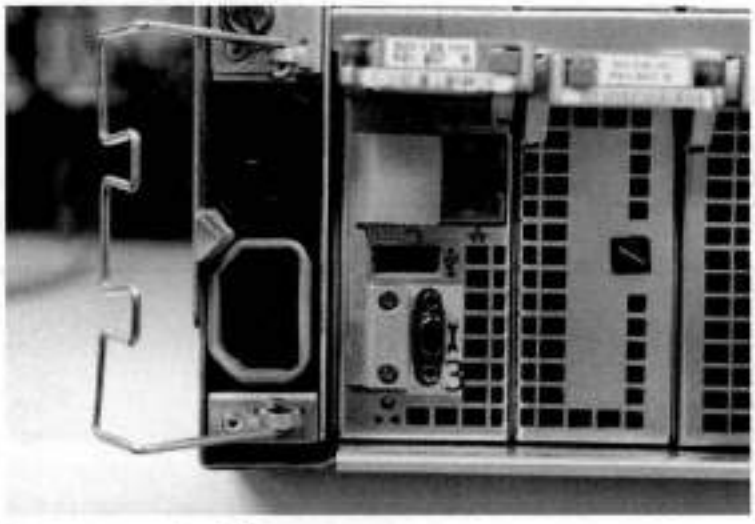


Figure 98. Interfaces on the management module

- 1 - Ethernet port
- 2 - USB port
- 3 - Micro serial port

I/O modules and slot assignments

The table shows the I/O module slot assignments for the systems. See Features on rear of chassis for a view of the slot positions on the back panel and Top view of SP module with SP cover removed for a top view.

Table 110. DD7200 slot assignments

Slot Number	DD7200	DD7200 with Extended Retention Software	DD7200 with DD Cloud Tier
MGMT A	Management module	Management module	Management module
0	Fibre Channel (FC), Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
1	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
2	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
3	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
4	Ethernet or empty	Ethernet or empty	Ethernet or empty
5	Ethernet or empty	SAS	SAS
6	Empty	SAS	SAS
7	SAS	SAS	SAS
8	SAS	SAS	SAS
9	BBU	BBU	BBU
10	NVRAM	NVRAM	NVRAM

Slot addition rules

- A maximum of six optional I/O modules (FC plus Ethernet) are allowed in systems without Extended Retention software, and a maximum of five optional I/O modules (FC plus Ethernet) are allowed in systems with Extended Retention software.
- Additional FC modules should be installed in numerically increasing slot numbers immediately to the right of the existing FC modules, or starting in slot 0 if no FC modules were originally installed. A maximum of four FC modules are allowed in a system.
- Additional Ethernet modules should be installed in numerically decreasing slot numbers immediately to the left of the existing Ethernet modules or starting in slot 4 if no Ethernet modules were originally installed. For systems without Extended Retention software, a maximum of six (limited to four of any one type) Ethernet modules can be present. For systems with Extended Retention software, a maximum of five (limited to four of any one type) Ethernet modules can be present.
- All systems include two SAS modules in slots 7 and 8. Systems with Extended Retention software must have two additional SAS modules in slots 5 and 6.
- For systems without Extended Retention software, if adding I/O modules results in the allowed maximum of six I/O modules present, slot 5 is used. Slot 5 is only used for an Ethernet module. Adding FC modules in this specific case require moving an existing Ethernet module to slot 5. Other than this specific case, it is not recommended to move I/O modules between slots.
- Adding Extended Retention software to a system includes adding two SAS modules in slots 5 and 6. If the system originally had the maximum of 6 optional I/O modules, the I/O module in slot 5 must be permanently removed from the system.

Fibre Channel (FC) I/O Module Option

An FC I/O module is a dual-port Fibre Channel module. The optional virtual tape library (VTL) feature requires at least one FC I/O module. Boost over Fiber Channel is optional and the total FC HBAs cannot exceed more than allowable Fibre Channel cards per controller.

Ethernet I/O Module Options

The available Ethernet I/O modules are:

- Dual Port 10GBase-SR Optical with LC connectors

- Dual Port 10GBase-CX1 Direct Attach Copper with SPF+ module
- Quad Port 1000Base-T Copper with RJ-45 connectors
- Quad port 2 port 1000Base-T Copper (RJ45) /2 port 1000Base-SR Optical

Internal system components

The photo shows the system with the system processor (SP) module that is removed from the chassis and the SP cover removed.

Figure 99. Top view of SP module with SP cover removed

- 1 - Front of system
- 2 - Four groups of 4 DIMM cards

DIMM modules

- DD7200 systems with 128 GB of memory contain 8 x 16 GB DIMMs, with 8 empty DIMM slots.
- DD7200 systems with 256 GB of memory contain 16 x 16 GB DIMMs.

DD7200 and ES30 shelf guidelines

The Data Domain system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your Data Domain system as listed in the following table below.
- Use the Installation and Setup Guide for your Data Domain system to minimize the chance of a cabling mistake.
- A Data Domain system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.
- ES30 SATA shelves must be on their own chain.

NOTE:

- ES30 SAS shelves must be running DD OS 5.4 or later.
- ES30-45 SATA shelves must be running DD OS 5.4 or later.
- DD OS 5.7 and later support 4TB drives.

Table 111. DD7200 and ES30 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	ES30 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB) [1]	Max RAW external capacity (TB) [2]
DD7200	128	2x4	SAS 30, 45; SATA 15, 30, 45[3]	5[4]	4	192	256
DD7200	256	2x4	SAS 30, 45, 60; SATA 15, 30, 45[3]	5[4]	4	384	540
DD7200 ER[5, 6]	256	4x4	SAS 30, 45, 60; SATA 15, 30, 45[3]	7	8	768	1024
DD7200 w/ DD Cloud Tier[7]	256	2x4	SAS 30, 45, 60; SATA 15, 30, 45[3]	5[4]	4	384 (max), additional 192 SAS dedicated to DD Cloud Tier	512 (max), additional 240 SAS dedicated to DD Cloud Tier

1. This figure only counts drives that have user data in the shelves.

2. The raw capacity of an ES30 is 125% of the available capacity.

3. ES30-45 (SATA) is only supported with DD OS 5.4 or later.

4. 5 shelves maximum with ES30, 4 is the recommended maximum. 4 shelves maximum with ES20, 3 is the recommended maximum.

5. With Extended Retention software.

6. The maximum shelf count for any specific drive/shelf size might be less than the product of max shelves x max shelves per set.

7. Only available with DD OS 6.0.

Single phase power connections for 40U-P (current racks)

The following figures show single phase power connections for several Data Domain systems.

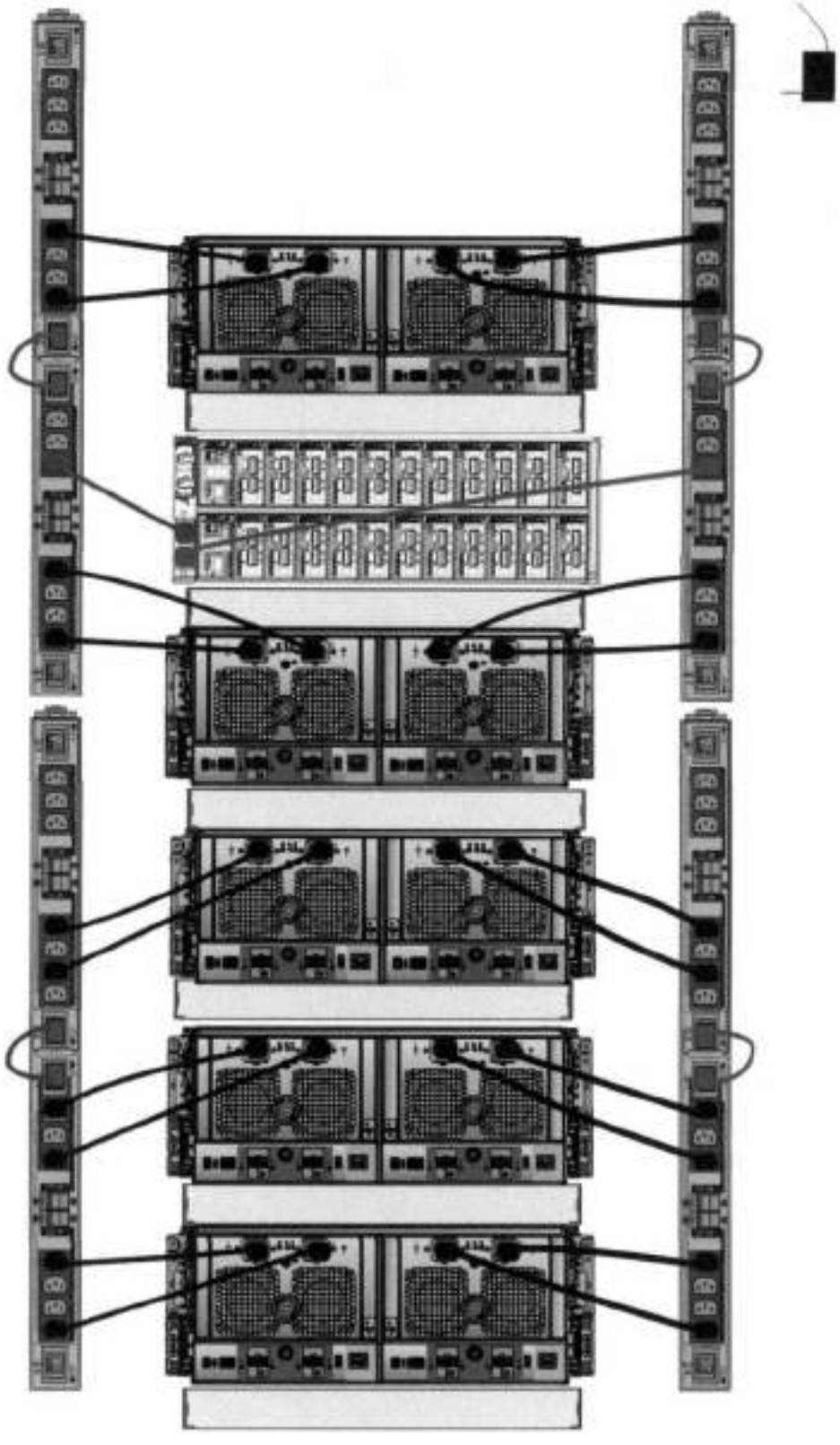


Figure 100. Single phase power connections for DD4200, DD4500, and DD7200 systems

Cabling shelves

ⓘ NOTE:

- Before cabling the shelves, physically install all shelves in the racks. Refer to the rail kit installation instructions included with the ES30 shelf for rack mounting.
- The documentation refers to two SAS HBAs. If only one HBA is allowed in a system, then use another port as defined later for that specific system.
- On an HA system, add cables from the second node to open ports at the end of the sets. The ports on the second node must connect to the same sets as the corresponding ports on the first node.

Ports on the system's SAS HBA cards connect directly to a shelf controller's host port. For redundancy, you need to create dual paths by using a port on one SAS HBA card to connect to one shelf controller in each shelf set, and a port on another SAS HBA card to connect to another shelf controller in the same shelf set. With dual paths, if one SAS HBA card fails, the shelf is still operational. However, in the unlikely event any single shelf becomes completely disconnected from power or SAS cables and becomes disconnected from a previously operational shelf, the file system goes down and the shelf is not operational. This is considered a double failure.

There are two kinds of configurations: one shelf in a set or multiple shelves in a set.

ES30 and DD7200 cabling

There are a few rules that must be followed when adding a mixture of ES20, ES30 SATA, and ES30 SAS shelves to your system. If a system does not follow ALL of these rules it is not a legitimate configuration.

Prerequisites:

- Follow the minimum and maximum shelf capacity configuration provided in the table.
- You cannot have ES20 and ES30 shelves in the same set.
- You cannot have ES30 SATA and ES30 SAS shelves in the same set.
- You cannot exceed the maximum amount of raw capacity displayed in the product's cabling table.
- The maximum number of shelves displayed in the product's cabling table cannot be exceeded.
- You cannot have more than four ES20s in a single set (maximum preference is three).
- You cannot have more than five ES30s in a single set (maximum preference is four).
- You can have a maximum of seven ES30s for systems with Extended Retention software.
- There are no specific placement or cabling requirements for the metadata shelves for DD Cloud Tier configurations. These shelves can be installed and cabled the same way as standard ES30 shelves.

NOTE: An ES20 requires more power than an ES30. Ensure that your rack is configured to handle the power needs.

The tables below show how to configure a mixed system. To use the tables, go to the appropriate system. Then find the number of ES20s that are to be configured in the first column. The next column defines the number of ES20 sets. If there are multiple rows with the same number of ES20s then pick the row with the appropriate number of ES20 SATA shelves. The next column in that row defines the number of sets of ES30 SATA shelves. Finally, there may be entries for the number of desired ES30 SAS shelves and the number of sets to be used.

If the combinations of shelves exceed the supported usable storage, there may not be an entry. The entries are based on the smallest usable storage per shelf type (12TB for ES20, 12 TB for ES30 SATA, and 24TB for ES30 SAS). Always check that the sum of the usable storage of all of the shelves does not exceed the supported usable storage of the configuration.

Table 112. Minimum and maximum configurations

System	Minimum appliance shelf count	Maximum appliance shelf count	DD Cloud Tier systems in TB	Extended Retention systems (ER) in TB	Max shelves for ER
7200 (384)	3	20	• 428 • 240 for metadata	• DD OS 5.4 and earlier: 1728 • DD OS 5.5 and later: 768	56

Systems without Extended Retention or DD Cloud Tier all support four chains. The following tables show combinations of ES20 and ES30 shelves. For combinations of any two types of shelves, these tables can be used as a guide.

Table 113. DD7200 cabling information

DD7200					
ES20	ES20 chains	ES30 SATA	ES30 SATA chains	ES30 SAS	ES30 SAS chains

Table 113. DD7200 cabling information (continued)

DD7200					
13-16	4	0	0	0	0
9-12	3	1-5	1	0	0
9-12	3	0	0	1-5	1
5-8	2	1-5	1	1-5	1
5-8	2	6-8	2	0	0
5-8	2	0	0	1-5	1
5-8	2	0	0	6-10	2
1-4	1	11-15	3	0	0
1-4	1	6-10	2	1-5	1
1-4	1	1-5	1	1-5	1
1-4	1	1-5	1	6-10	2
1-4	1	0	0	1-5	1
1-4	1	0	0	6-10	2
1-4	1	0	0	11-15	3
0	0	16-20	4	0	0
0	0	11-15	3	1-5	1
0	0	6-10	2	1-5	1
0	0	6-10	2	6-10	2
0	0	1-5	1	1-5	1
0	0	1-5	1	6-10	2
0	0	1-5	1	11-15	3
0	0	0	0	1-4	1
0	0	0	0	5-8	2
0	0	0	0	9-12	3
0	0	0	0	13-16/18	4

The following figures show cabling for base systems, systems with the Extended Retention software option, and systems integrated with an Avamar system.

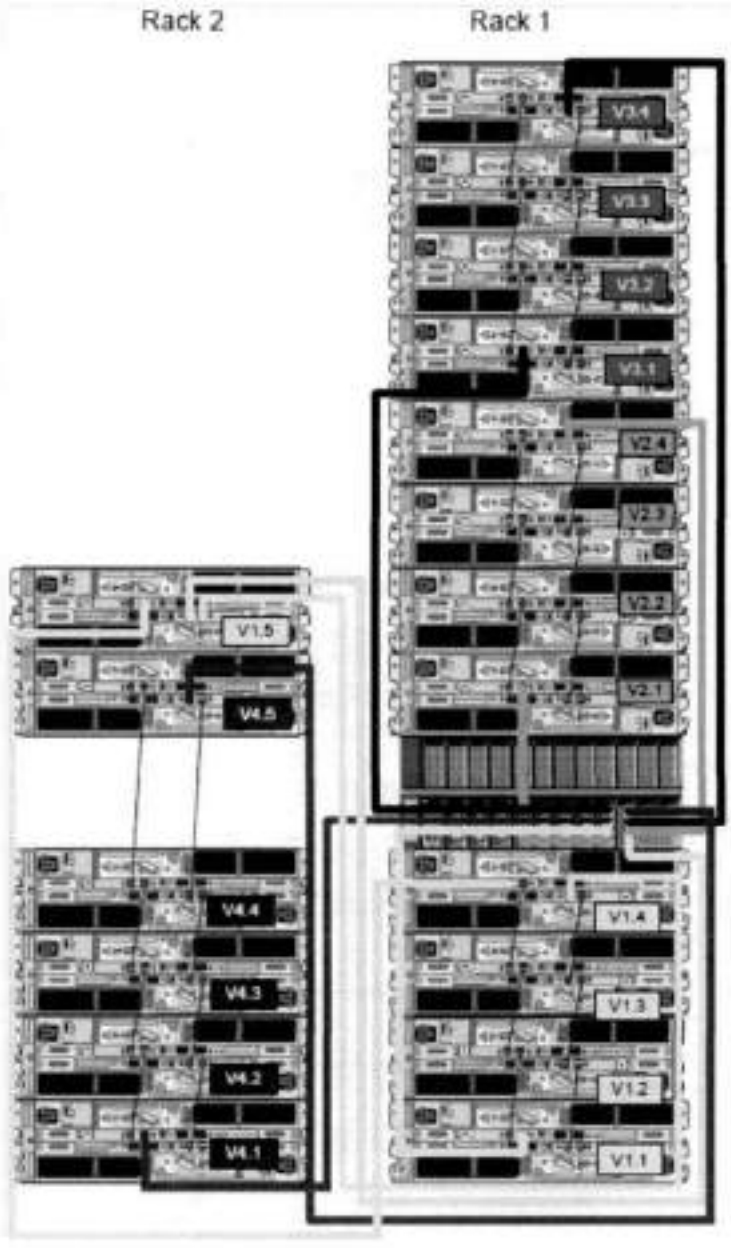


Figure 101. Recommended DD7200 cabling

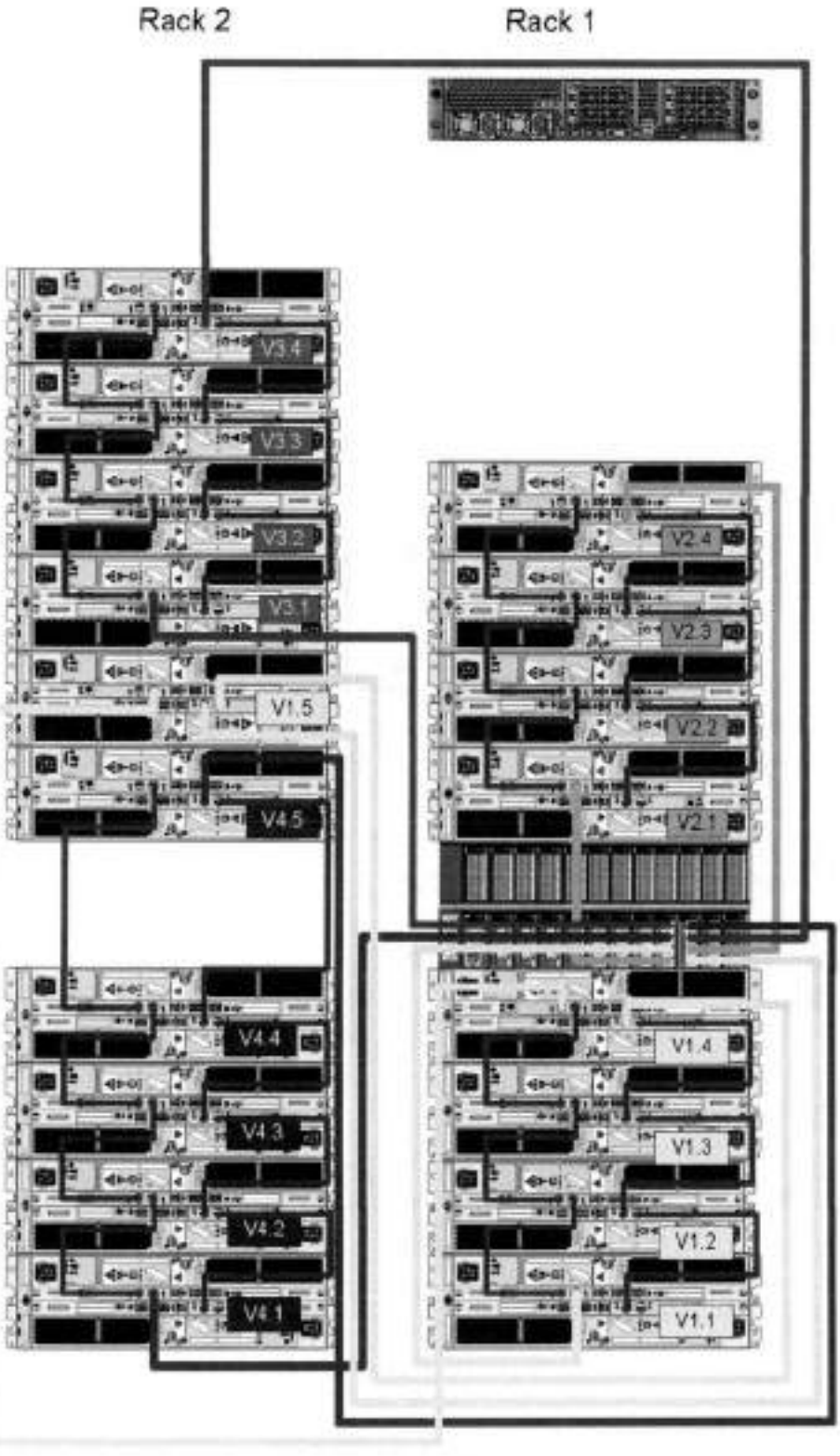


Figure 102. Recommended cabling for DD7200 integrated with Avamar

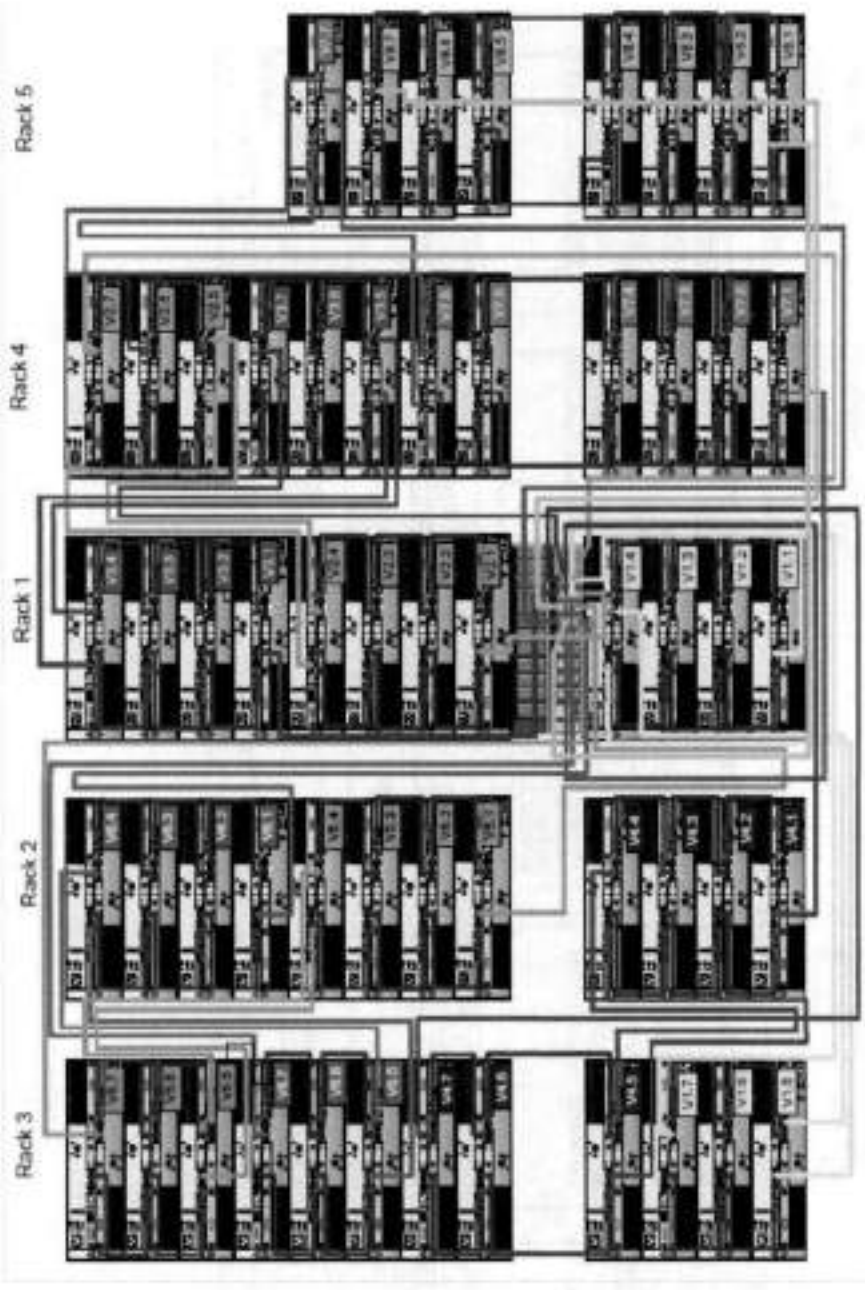


Figure 103. Recommended cabling for DD7200 with extended retention software or DD Cloud Tier

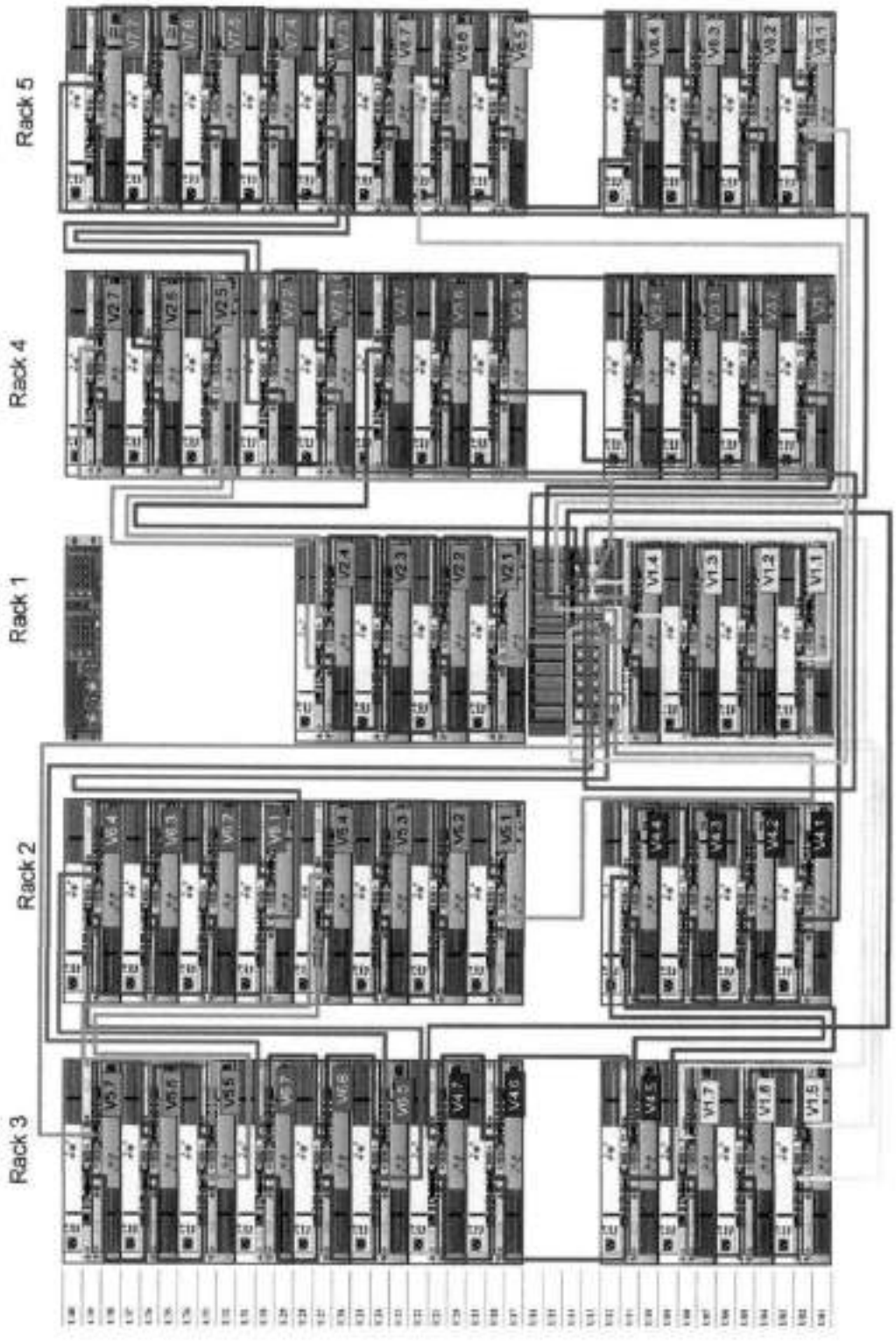


Figure 104. Recommended cabling for DD7200 with extended retention and integrated with Avamar

DD7200 and DS60 shelf guidelines

The Data Domain system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your Data Domain system as listed in the following table.
- For redundancy, the two connections from a Data Domain system to a set of shelves must use ports on different SAS I/O modules.
- Use the Installation and Setup Guide for your Data Domain system to minimize the chance of a cabling mistake.
- A Data Domain system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.
- ES30 SATA shelves must be on their own chain.
- If ES30 SAS shelves are on the same chain as a DS60, the maximum number of shelves on that chain is 5.
- DD OS 5.7.1 does not support HA with SATA drives.

Table 114. DD7200 and DS60 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	DS60 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB)[1]	Max RAW external capacity (TB)
DD7200	128	2x4	SAS 45	2	4	288	360
DD7200	256	2x4	SAS 45, 60	2	4	432	540
DD7200 ER [2]	256	4x4	SAS 45, 60	2	8	864	1080

NOTE: An entry of 45 corresponds to DS60-3 models and an entry of 60 corresponds to DS60-4 models.

1. This column only counts drives that have user data in the shelves. For example, a DS60 4-240 has 192TB.

2. With Extended Retention software.

Single phase power connections for 40U-P (current racks)

The following figures show single phase power connections for several Data Domain systems.

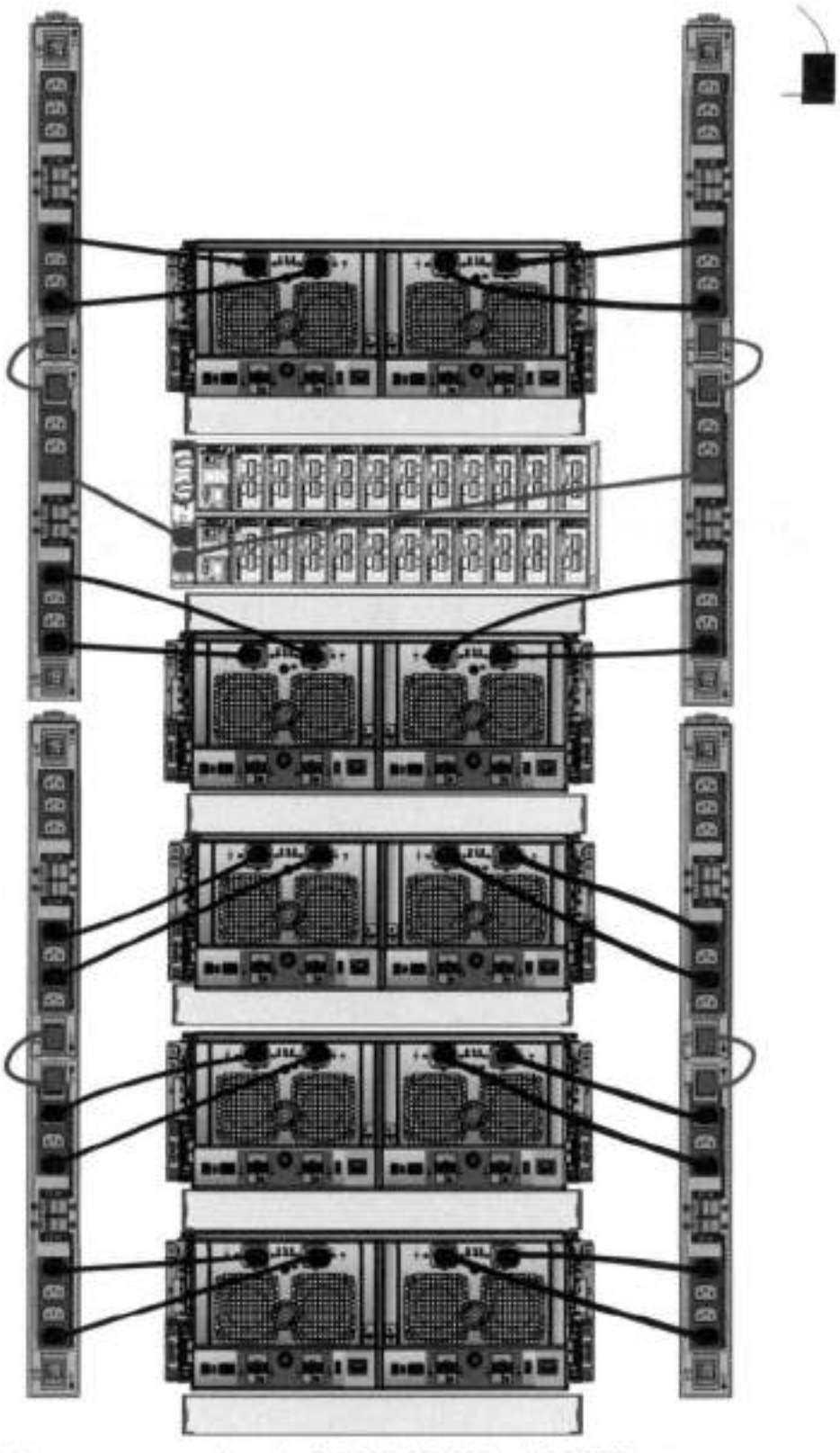


Figure 105. Single phase power connections for DD4200, DD4500, and DD7200 systems

3-phase power connections for 40U-P (current racks)

Some environments use 3-phase power for 40U-P racks used for several Data Domain systems. In those situations it is desirable to balance the current draw across all 3 phases. The recommended 3-phase power cabling attempts to do that, but an optimal

configuration is dependent on the specific installation. The following figures show recommended 3-phase power connections for several Data Domain systems.

NOTE: The next few diagrams show recommended 3-phase delta power connections.

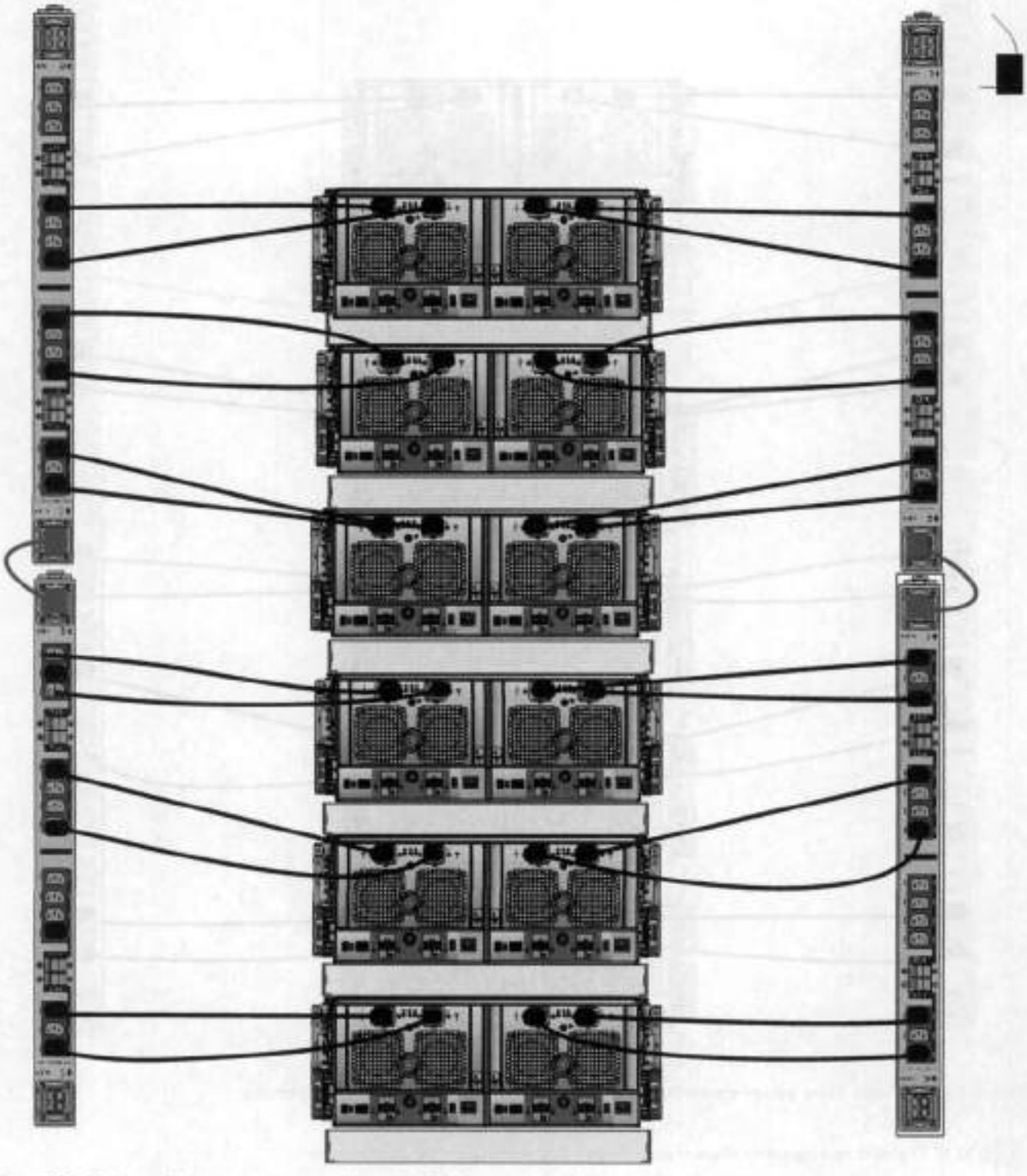


Figure 106. 3-phase delta power connections for DS60 expansion shelves (full-racked)

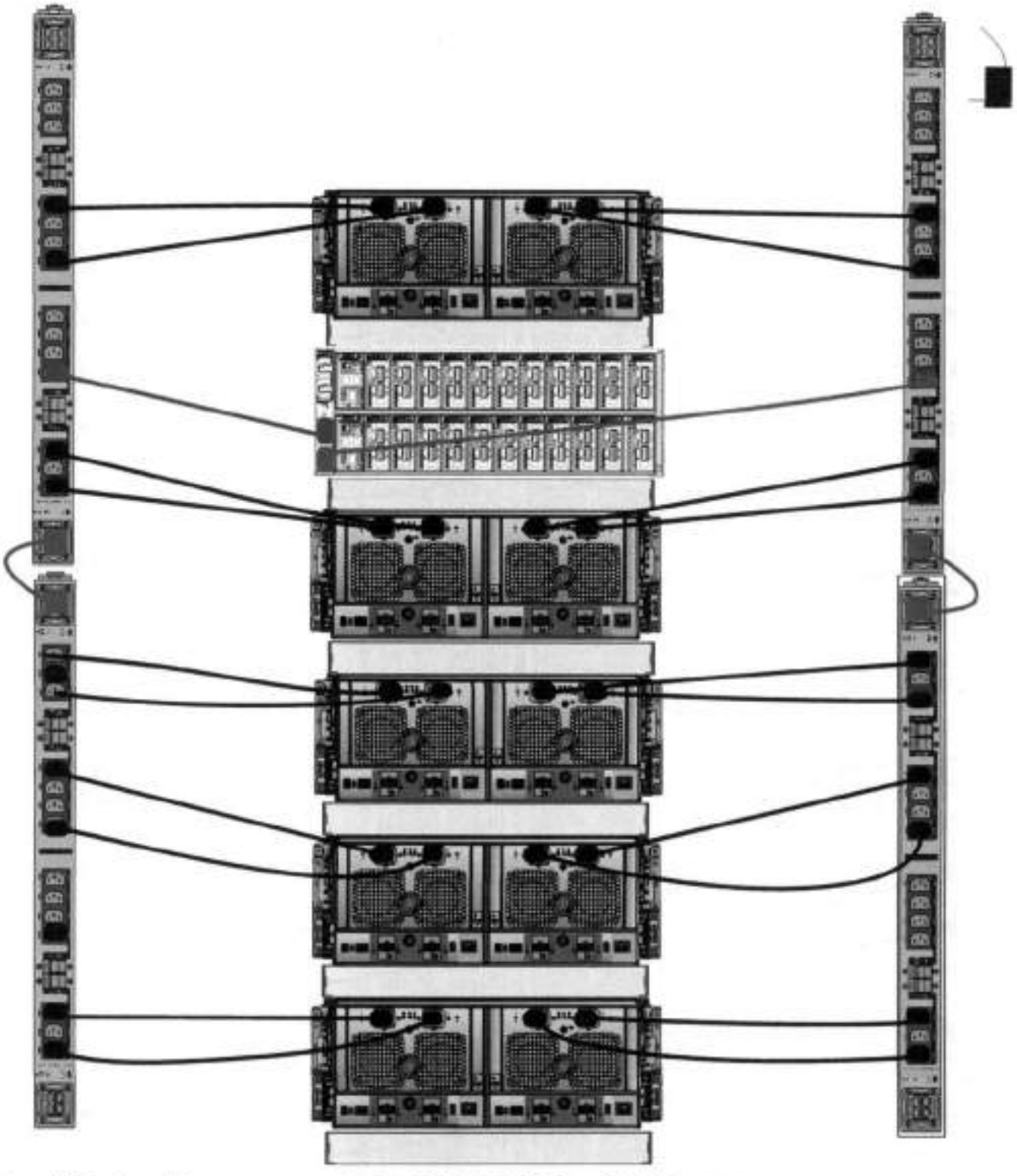


Figure 107. 3-phase delta power connections for DD4200, DD4500, and DD7200 systems

NOTE: The next few diagrams show recommended 3-phase wye power connections.

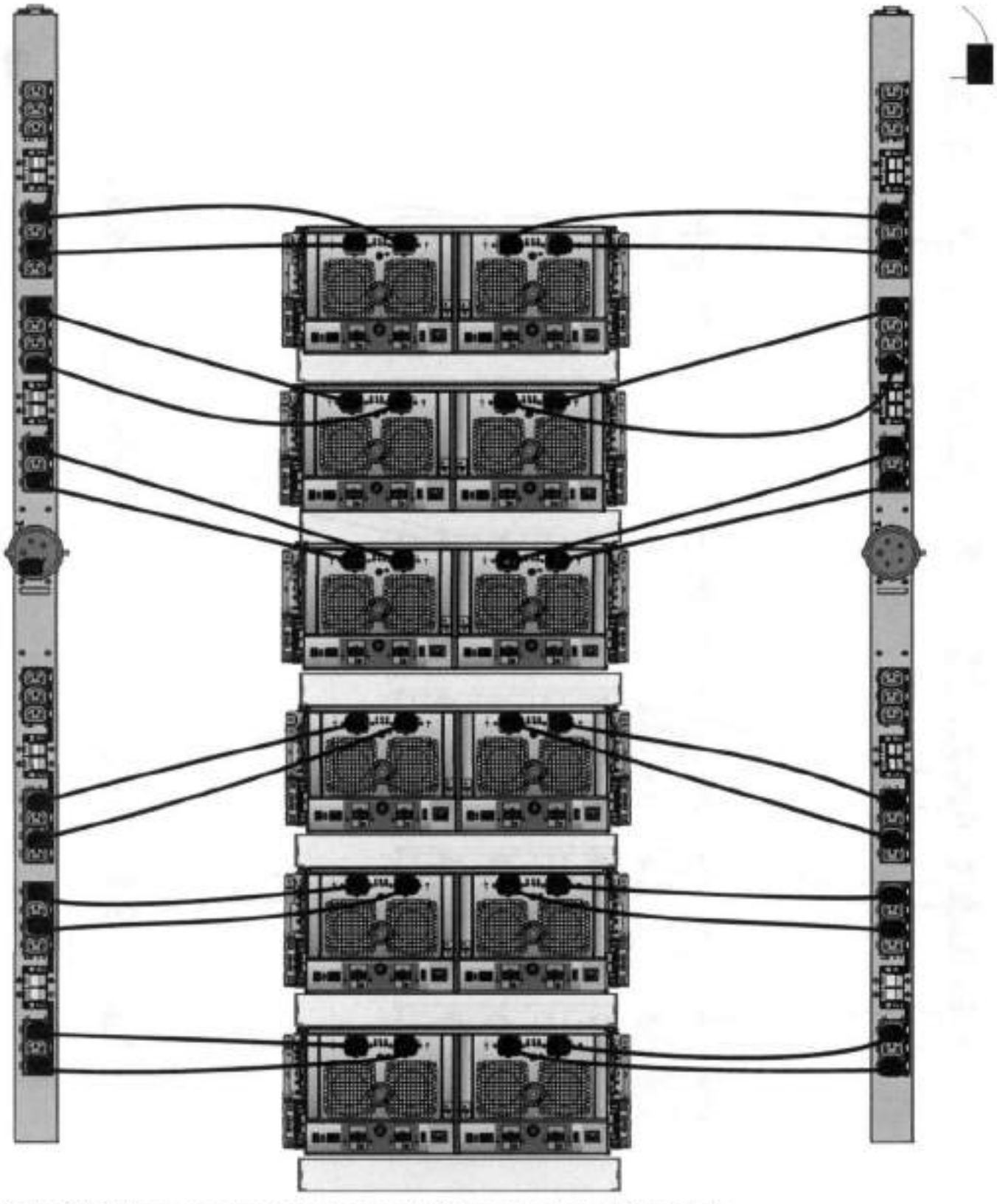


Figure 108. 3-phase wye power connections for DS60 expansion shelves (full-racked)

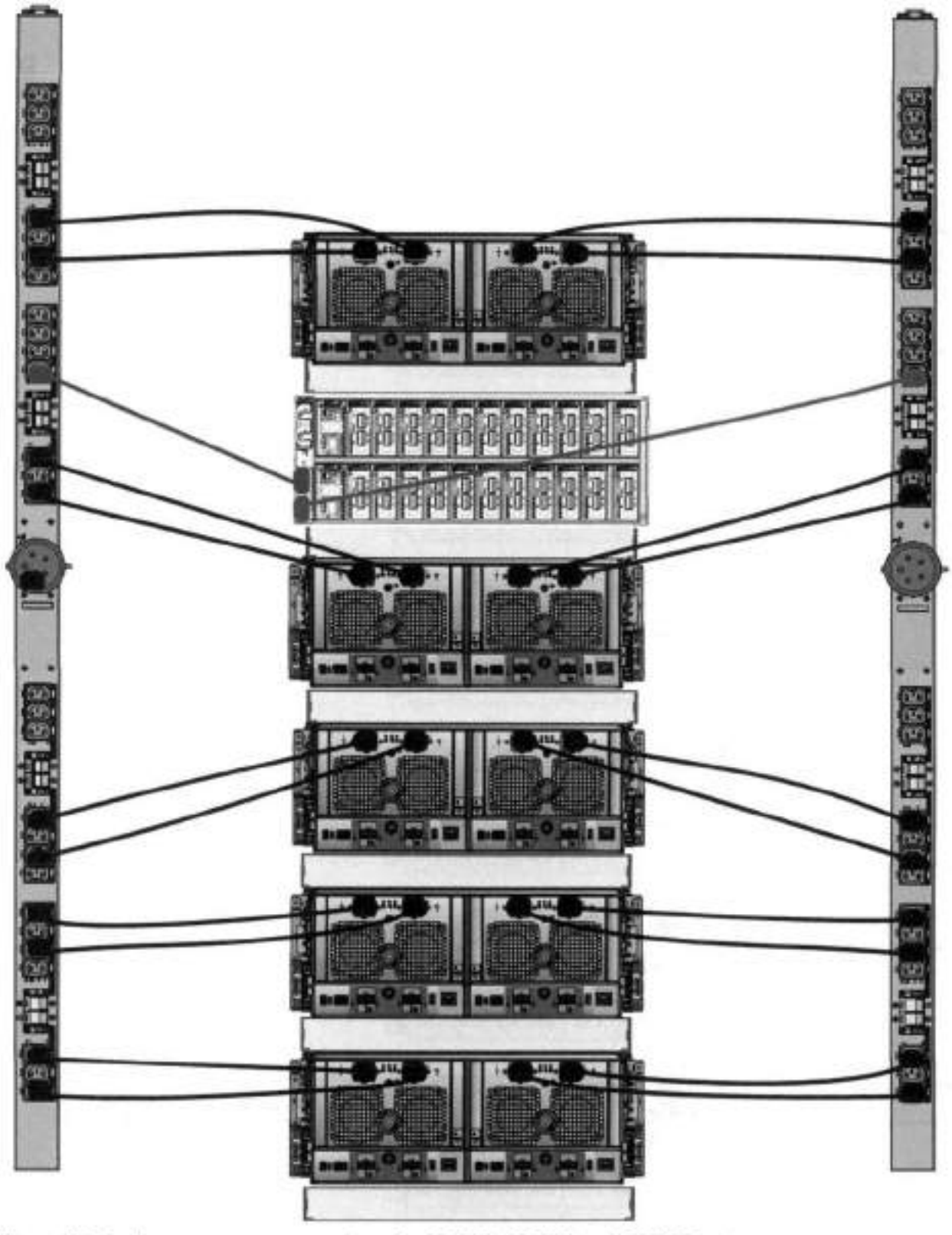


Figure 109. 3-phase wye power connections for DD4200, DD4500, and DD7200 systems

DS60 and DD7200 cabling

There are a few rules that must be followed when adding a mixture of DS60 and other shelf types to your system.

CAUTION: **If a system does not follow all these rules, it is not a legitimate configuration.**

Prerequisites:

- You cannot exceed the maximum amount of usable capacity displayed in cabling table for each system.
- You cannot exceed the maximum number of shelves displayed in cabling table for each system.
- You cannot connect more than two DS60 shelves in a single set.

Table 115. Minimum and maximum configurations

System	Appliance maximum	Minimum appliance shelf count
DD7200	384 TB	1

Mixing DS60, ES30, and ES20 shelves:

The non-Extended Retention versions of these systems all support four chains.

Extra planning and reconfiguration may be required to add DS60 shelves to system with ES20 shelves, ES30 SATA shelves, or a combination of shelves.

- The ES20 shelves must be on their own set. Minimize the ES20 set count by combining up to four ES20s per set.
- ES30 SATA shelves must also be on their own sets. Minimize the ES30 set count by combining up to five ES30s per set. If required, combine up to seven ES30 SAS shelves per set to minimize the set count.
- A set can contain a maximum of two DS60 shelves and, if required because of other restrictions, add ES30 SAS shelves up to a maximum of five shelves in that set.

NOTE: The configuration rules apply also to Extended Retention systems.

The following figures show cabling for base systems and systems with the Extended Retention software.

NOTE: It is recommended that the DS60 shelf with the greater number of drives should always be placed in the bottom position.

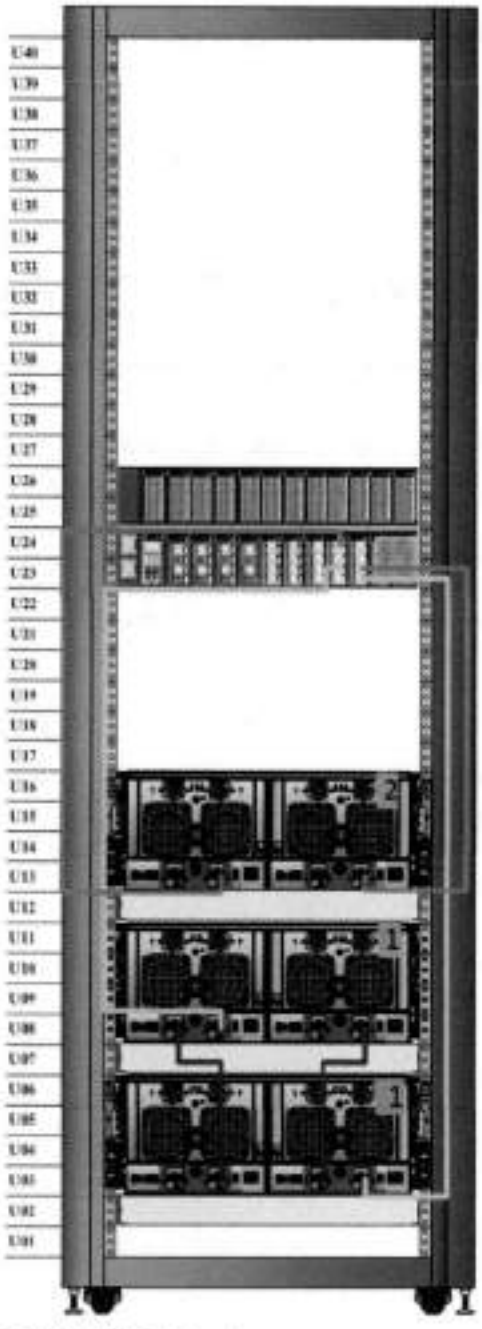


Figure 110. Recommended cabling for DD7200 (3TB drives)

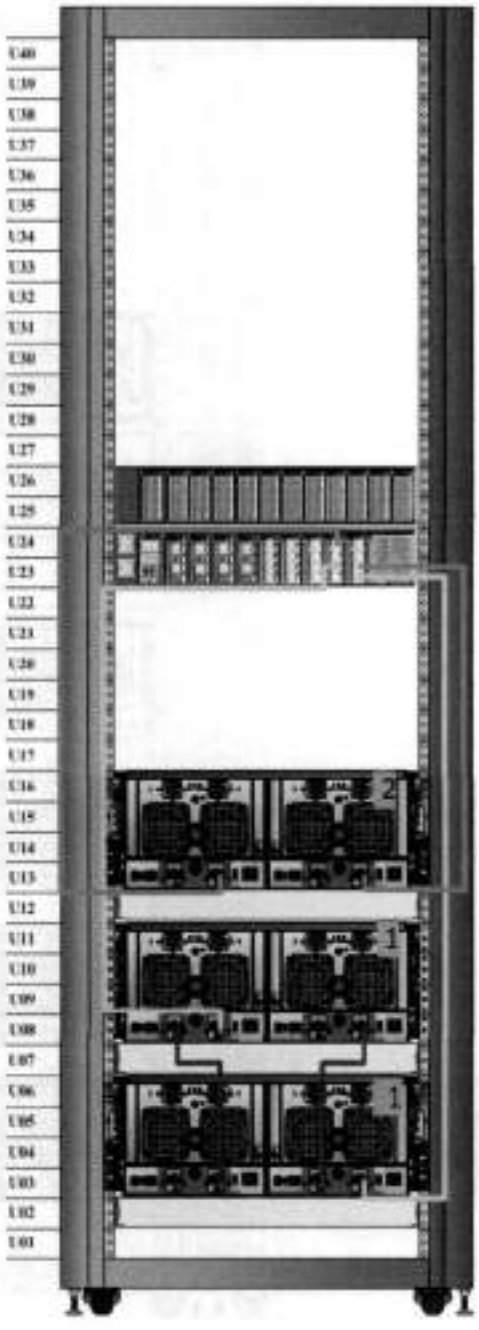


Figure 111. Recommended cabling for DD7200 (4TB drives)

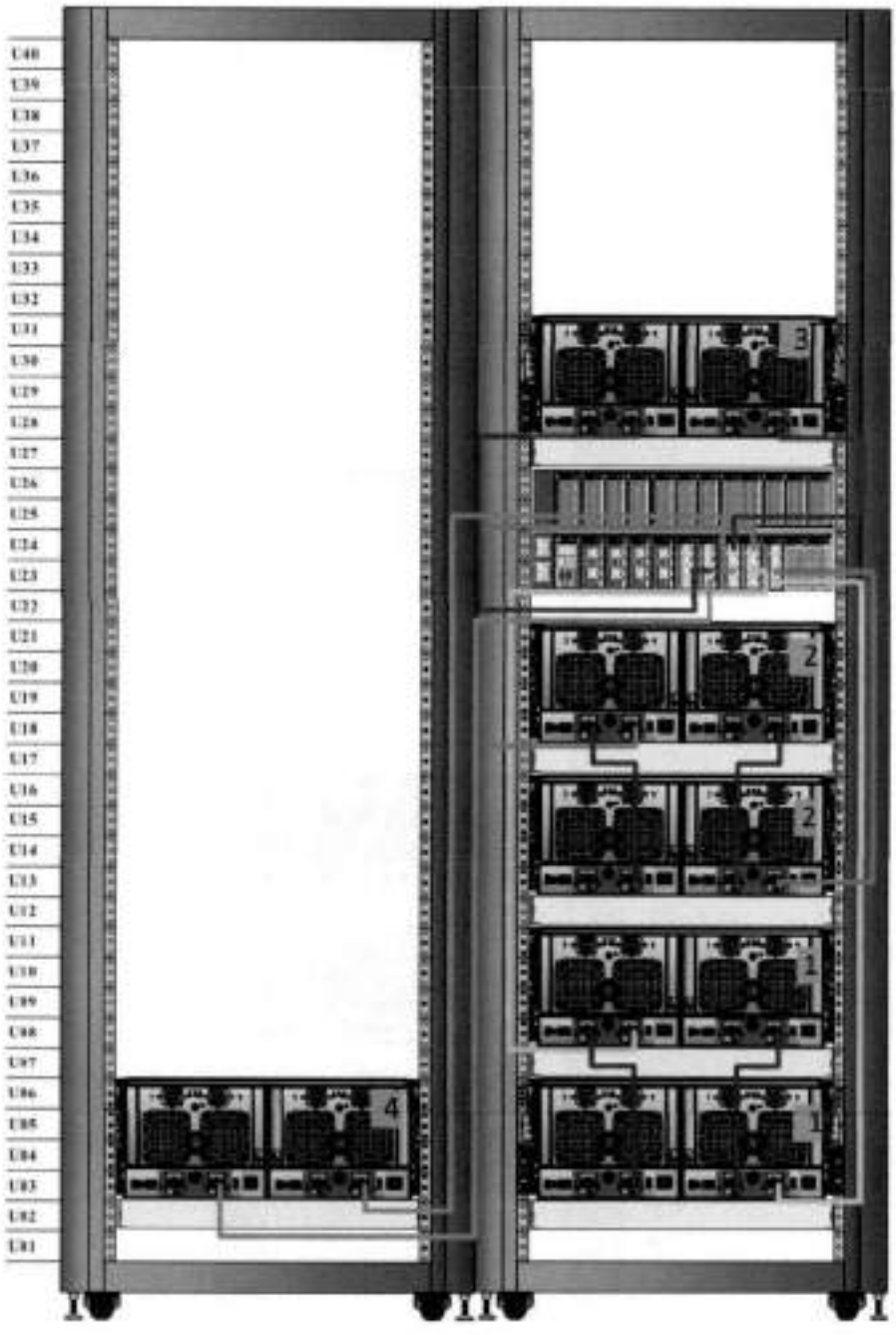


Figure 112. Recommended cabling for DD7200 (3TB drives) with Extended Retention software

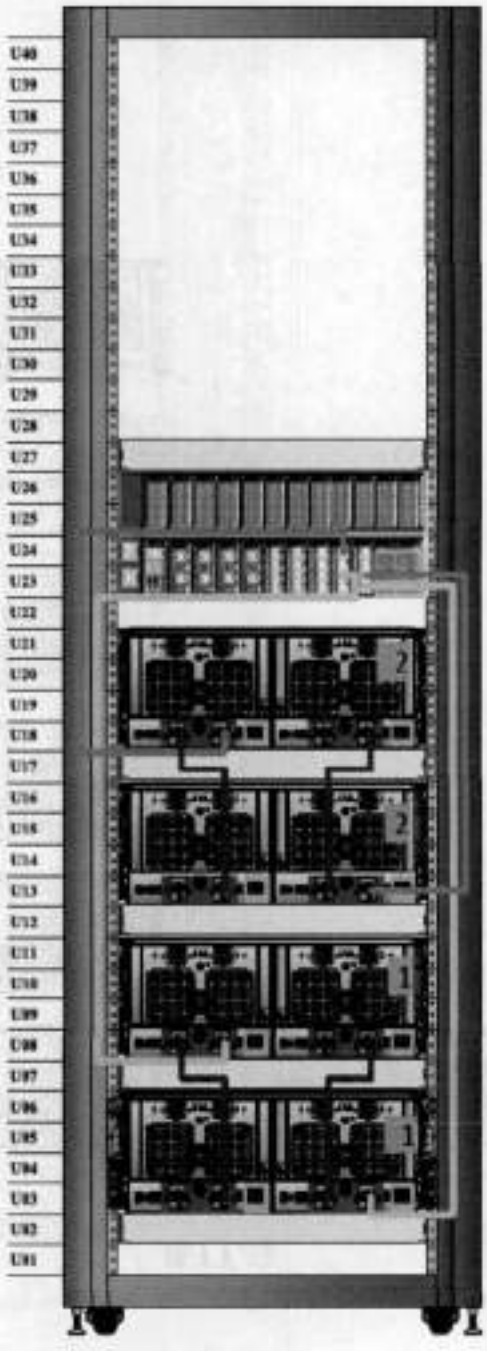


Figure 113. Recommended cabling for DD7200 with DD Cloud Tier

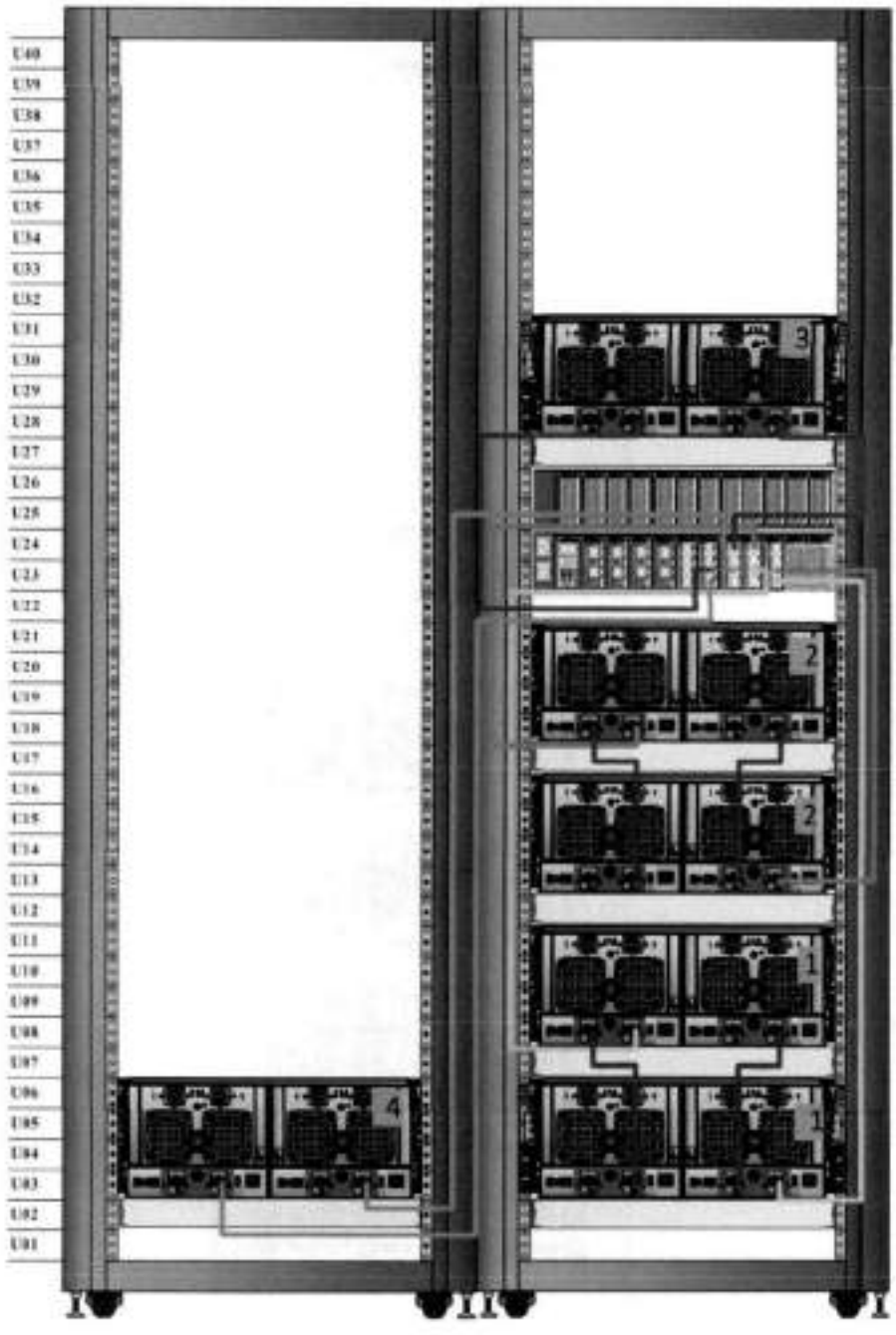


Figure 114. Recommended cabling for DD7200 (4TB drives) with Extended Retention software

10

DD9300

This chapter contains the following topics:

Topics:

- system features
- system specifications
- DD9300 storage capacity
- DD9300 front panel
- Back panel
- I/O modules
- Internal system components
- DD9300 and ES30 shelf guidelines
- DD9300 and DS60 shelf guidelines

system features

Table 116. system features

Feature		(Base configuration)	(Expanded configuration)
Rack height		2U	2U
Processor		E5-2680 V3	E5-2680 V3
Kernel		3.2.x	3.2.x
NVRAM		NVRAM 8g Model 3	NVRAM 8g Model 3
Memory		4 x 32 GB DIMM + 4 x 16 GB DIMM (192 GB)	8 x 32 GB DIMM + 8 x 16 GB DIMM (384 GB)
Internal drives	HDDs in 3.5" bays	4	4
	SSDs in 3.5" bays	5	8
	SSDs in 2.5" bays	0	0
I/O module slots	SAS I/O modules (Quad Port 6 Gbps SAS)	2	2
	Network and FC I/O modules	Four replaceable I/O module slots. Not hot-swappable.	Four replaceable I/O module slots. Not hot-swappable.
Supported capacity	Non-extended retention	384 TB	720 TB
	DD Cloud Tier	N/A	1440 TB [a]
	Extended retention	N/A	720 TB[b]
High availability support		Yes	Yes
HA private interconnect		(2) 10GBase-T ports	(2) 10GBase-T ports
External SSD shelf		One SSD shelf for A-P high availability cluster containing two drives.	One SSD shelf for A-P high availability cluster containing four drives.

Table 116. system features (continued)

Feature		(Base configuration)	(Expanded configuration)
SAS string depth (max)	ES30	6	6 (7 for extended retention)
	DS60	3	3
	ES30 and DS60	5 shelves total	5 shelves total
Stream count		810 writes, 225 reads	810 writes, 225 reads

a. DD Cloud Tier requires four ES30 shelves fully populated with 4 TB drives to store DD Cloud Tier metadata.
b. Extended retention not available on HA configurations

system specifications

Table 117. system specifications

Model	Average power consumption 25 C	Heat dissipation (operating maximum)	Weight [a]	Width	Depth	Height
	645W	1.69 x 10^6 J/hr (1604 Btu/hr) maximum	70 lbs (31.75 kg)	17.50 in (44.45 cm)	30.5 in (77.5 cm)	3.40 in (8.64 cm)

a. The weight does not include mounting rails. Allow 2.3-4.5 kg (5-10 lb) for a rail set.

Table 118. System operating environment

Requirement	Description
Ambient temperature	10°C - 35°C; derate 1.1°C per 1,000 ft (304 m)
Relative humidity (extremes)	20–80% noncondensing
Elevation	0 - 7,500ft (0 - 2,268m)
Operating acoustic noise	L_{wad} sound power, 7.5 Bels

DD9300 storage capacity

The following table provides storage capacity information for the DD9300 system.

Table 119. DD9300 storage capacity

Memory	Internal disks (system disks only)	External storage (raw)	Usable data storage space (TB/TiB/GB/GiB)[a]			
192 GB (Base)	• 4 x 4 TB HDD • 5 x 800 GB SSD	480 TB[b]	384 TB	349.2 TiB	384,000 GB	357,628 GiB
384 GB (Expanded)	• 4 x 4 TB HDD • 8 x 800 GB SSD	• Active Tier: 900 TB[b] • Archive Tier: 900 TB[c] • Cloud Tier: 1800 TB in the cloud[d]	• Active Tier: 720 TB • Archive Tier: 720 TB • Cloud Tier: 1,440 TB	• Active Tier: 654.8 TiB • Archive Tier: 654.8 TiB • Cloud Tier: 1,309.6 TiB	• Active Tier: 720,000 GB • Archive Tier: 720,000 GB • Cloud Tier: 144,000 GB	• Active Tier: 670,552 GiB • Archive Tier: 670,552 GiB • Cloud Tier: 1,341,104 GiB

Table 119. DD9300 storage capacity (continued)

Memory	Internal disks (system disks only)	External storage (raw)	Usable data storage space (TB/TiB/GB/GiB)*			
		• Cloud Tier metadata: 240 TB local storage	• Cloud Tier metadata: 192 TB	• Cloud Tier metadata: 174.6 TiB	• Cloud Tier metadata: 192,000 GB	• Cloud Tier metadata: 178,814 GiB

a. The capacity differs depending on the size of the external storage shelves used. This data based on ES30 shelves.
b. HA is supported.
c. HA is not supported with Extended Retention.
d. HA is supported in combination with Cloud Tier.

DD9300 front panel

DD9300 Dataless Head (DLH) systems have one of the following front panel drive configurations to host the DD OS boot drives and provide metadata caching on SSD.

Table 120. DD9300 DLH SSD requirements

Configuration	Number of SSDs
DD9300	5
DD9300 expanded	8
NOTE: SSDs are not RAID-protected.	

Table 121. DD9300 DLH configuration drive layout

Slot 0: HDD 1	Slot 1: HDD 2	Slot 2: HDD 3	Slot 3: HDD 4
Slot 4: SSD 1	Slot 5: SSD 2	Slot 6: SSD 3	Slot 7: SSD 4
Slot 8: SSD 5	Slot 9: Filler	Slot 10: Filler	Slot 11: Filler

Table 122. DD9300 DLH expanded configuration drive layout

Slot 0: HDD 1	Slot 1: HDD 2	Slot 2: HDD 3	Slot 3: HDD 4
Slot 4: SSD 1	Slot 5: SSD 2	Slot 6: SSD 3	Slot 7: SSD 4
Slot 8: SSD 5	Slot 9: SSD 6	Slot 10: SSD 7	Slot 11: SSD 8

Front LED indicators

The front of the system contain 12 disk drive status LEDs that are normally blue, and blink when there is activity on the disk. The LEDs are shaped like triangles, and the apex of the triangle points left or right, indicating that disk's status. If the disk drive has a failure, the disk's status LED turns from blue to amber, indicating that a drive must be replaced.

The front also contains two system status LEDs. A blue system power LED is present that is on whenever the system has power. An amber system fault LED is also present that is normally off and lit amber whenever the chassis or any other FRU in the system requires service.

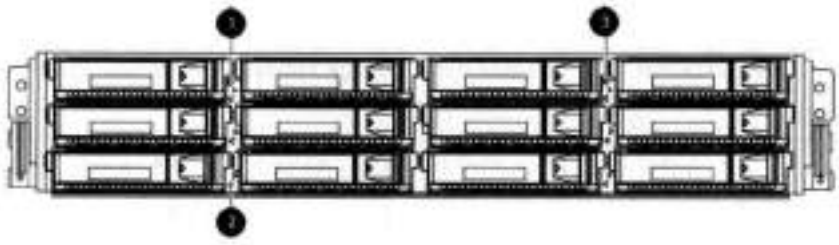


Figure 115. Front LED indicators

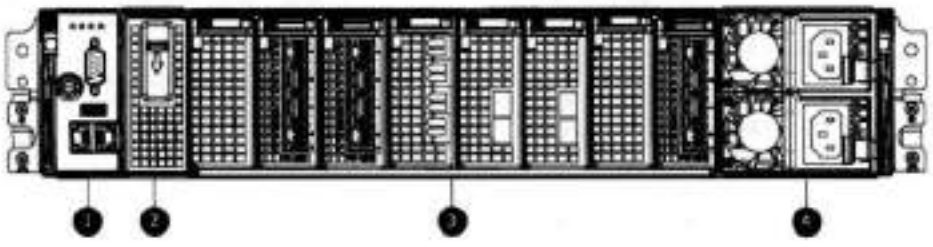
1. System service LED
2. Drive activity/service LED
3. System power LED

Table 123. Front LEDs

Name	Color	Purpose
System power LED	Blue	Indication that the system has power.
System service LED	Amber	Normally off; is lit amber whenever the SP or any other FRU (except disk drives) in the system requires service.
Drive activity/Service LED	Blue /Amber	• Lit blue when the drive is powered. • Blinks blue during drive activity. • Lit solid amber when a disk needs service.

Back panel

The back panel of the chassis contains the following components:



1. Management panel
2. Not Used -- Two 2.5" SSD slots labeled 0 and 1
3. I/O module slots
4. Power supply modules (PSU 0 is the lower module, and PSU 1 is the upper module)

Rear LED indicators

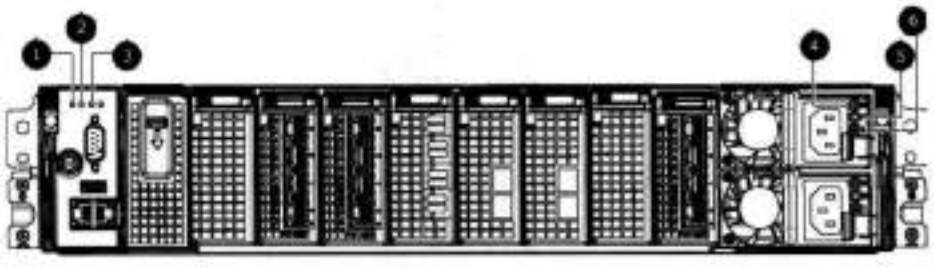


Figure 116. Rear LED indicators

1. Do not remove LED
2. SP service LED
3. System power LED
4. AC power good LED
5. DC power good LED
6. Power supply fault LED

Name of LED	Location	Color	Definition
"Do not remove" LED	Upper left-most part of rear chassis	White	This LED is lit during system BIOS and BMC firmware updates and indicates that the SP should not be removed from the chassis, nor should system power be removed.
SP service LED	To the right of "Do not remove" LED	Amber	• Solid amber - SP or a FRU inside the SP requires service • Blinking amber - blink rate reflects one of the following is booting ○ BIOS - 1/4 Hz ○ POST - 1 Hz ○ OS - 4 Hz
Drive Power/Activity LED [a]	Left LED on the SSD	Blue	Lit blue when the drive is powered. Blinks during drive activity.

Name of LED	Location	Color	Definition
Drive Fault LED[a]	Right LED on the SSD	Amber	Lit solid amber when a drive needs service.
System power LED	Right-most LED on the management panel	Blue	SP has good, stable power
PSU FRU LED - AC Good	Top LED on power supply	Green	AC input is as expected
PSU FRU LED - DC Good	Middle LED on power supply	Green	DC output is as expected
PSU FRU LED - Attention	Bottom LED on power supply	Amber	PSU has encountered a fault condition

a. The SSD is only present on DD6300 systems.

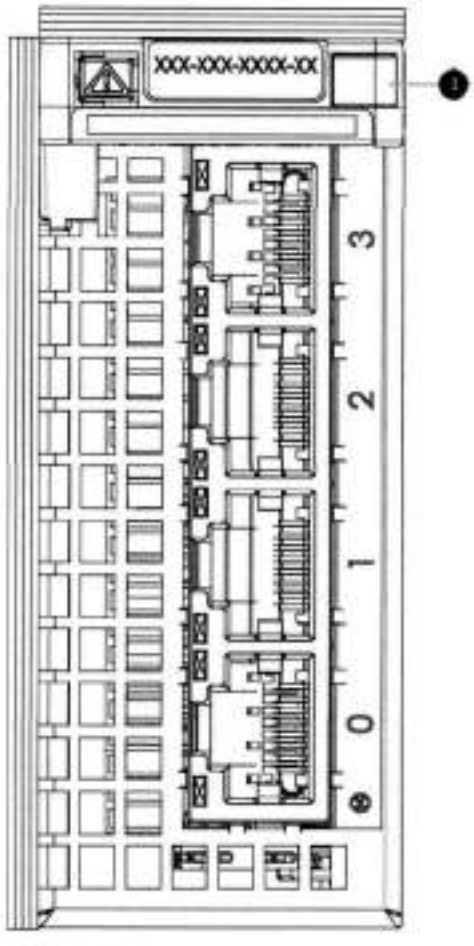


Figure 117. I/O module Power/Service LED location

1. I/O module power/service LED

Table 124. I/O LEDs

Name of LED	Location	Color	Definition
I/O module FRU LED - I/O module Power/Service LED location	Ejector handle of I/O modules	Green/Amber	• Green - I/O module has power and is functioning normally • Amber - I/O module has encountered a fault condition and requires service

Table 124. I/O LEDs (continued)

Name of LED	Location	Color	Definition
I/O port status LED (SAS, Fibre Channel, and optical networking I/O modules only)	One LED per I/O module port	Blue	Lit when port is enabled. May flash if SW "marks" the port. [a]

a. For RJ45 networking ports, the standard green link and amber activity LEDs are used.

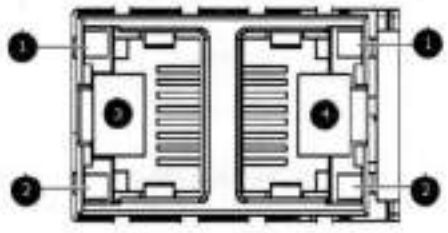


Figure 118. Onboard network port LEDs

1. Network port link LED
2. Network port activity LED
3. Dedicated IPMI port BMC0A
4. Management interface Eth0a

Table 125. Onboard network port LEDs

Name of LED	Location	Color	Definition
Onboard network port LED - Link LED Onboard network port LEDs	Top LED on network port	Green	• Lit when there is a link at 1000BaseT and 100BaseT speeds • Off when the link speed is 10BaseT or there is no link
Onboard network port LED - Activity LED	Bottom LED on network port	Amber	Blinks when there is traffic on the port

I/O modules

I/O module slot numbering

The eight I/O module slots are enumerated as Slot 0 (on the left when viewed from the rear) through Slot 7. Ports on an I/O module are enumerated as 0 through 3, with 0 being on the bottom.

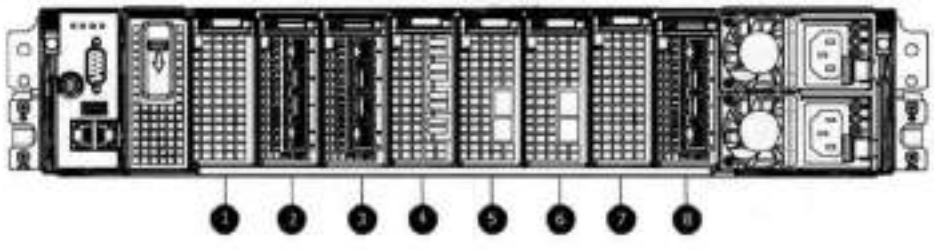


Figure 119. I/O module slot numbering

1. Slot 0
2. Slot 1
3. Slot 2

4. Slot 3
5. Slot 4
6. Slot 5
7. Slot 6
8. Slot 7

I/O modules are only supported in fixed configurations. The fixed configurations define the exact slots into which the I/O modules may be inserted. The processors directly drive the eight I/O module slots, meaning all slots are full performance.

The non-optional SAS, NVRAM, and 10GBaseT I/O modules are allocated to fixed slots. The optional Host Interface I/O modules are used for front end networking and Fibre Channel connections. The quantity and type of these I/O modules is customizable, and there are many valid configurations.

slot map

I/O module slots 3–6 contain optional Host Interface I/O modules and can contain specific I/O modules or no I/O modules at all. Slot 0, Slot 1, Slot 2, and Slot 7 are populated with the required I/O modules and are not optional.

Table 126. I/O module slot mapping

Tier	Slot 0	Slot 1	Slot 2	Slot 3	Slot 4	Slot 5	Slot 6	Slot 7
DLH DLH Extended Retention/DD Cloud Tier	NVRAM 8g Model 3	Quad Port 10 GBase-T	Quad Port 6 Gbps SAS	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 6 Gbps SAS
DLH High Availability	NVRAM 8g Model 3	Quad Port 10 GBase-T for HA interconnect	Quad Port 6 Gbps SAS	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 10GbE SR, Quad Port 10 GBase-T, or Dual Port 16 Gbps Fibre Channel	Quad Port 6 Gbps SAS

I/O module population rules

The system chassis has eight slots for I/O modules. Slots 0, 1, 2, and 7 are reserved. Slots 3, 4, 5, and 6 support host interface I/O modules. The maximum supported number of any type of host interface I/O module is four.

NOTE: A maximum of three Quad Port 10 GBase-T I/O modules are supported in slots 3-6 because of the mandatory Quad Port 10 GBase-T I/O module in slot 1.

The following table assigns rules for populating the I/O modules.

Table 127. I/O module slot population rules

Step	I/O module name	Slots	Notes
Step 1: Populate mandatory I/O modules	NVRAM 8g Model 3	0	Mandatory for all configurations
	Quad Port 10 GBase-T	1	Mandatory for all configurations
	Quad Port 6 Gbps SAS	2	Mandatory for all configurations
	Quad Port 6 Gbps SAS	7	Mandatory for all configurations

Table 127. I/O module slot population rules (continued)

Step	I/O module name	Slots	Notes
Step 2: Populate all Quad Port 10GbE SR I/O modules	Quad Port 10GbE SR	3, 4, 5, 6	Populate starting from the lowest available slot number.
Step 3: Populate all Quad Port 10 GBase-T I/O modules	Quad Port 10 GBase-T	3, 4, 5, 6	Populate starting from the lowest available slot number. With Quad Port 10 GBase-T in slot 1, max number of Quad Port 10 GBase-T I/O modules are limited to 4.
Step 4: Populate all Dual Port 16 Gbps Fibre Channel I/O modules	Dual Port 16 Gbps Fibre Channel	6, 5, 4, 3	Populate starting from the highest available slot number.

Internal system components

The following figure shows the layout of the CPUs and DIMMs inside the chassis. The front of the system is at the top of the figure.

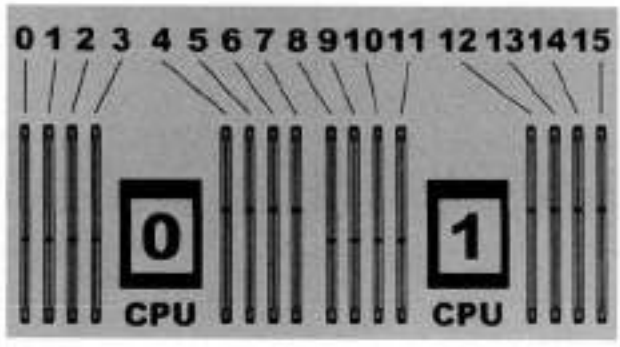


Figure 120. CPU and memory locations

DIMMs overview

Dual in-line memory modules (DIMM) come in various sizes, which must be configured in a certain way. This topic can help you select the correct configuration when servicing DIMMs.

The storage processor contains two Intel processors each with an integrated memory controller that supports four channels of memory. The storage processor allows two DIMM slots per channel, so the storage processor supports a total of 16 DIMM slots.

memory DIMM configuration

Table 128. memory DIMM configuration

Tier	Total Memory	Memory DIMM Configuration
DLH Expanded	384 GB	8 x 32 GB + 8 x 16 GB
DLH	192 GB	4 x 32 GB + 4 x 16 GB
DLH Extended Retention/DD Cloud Tier	384 GB	8 x 32 GB +8 x 16 GB

HA is supported with all available memory configurations.

To ensure maximum memory performance, there are memory DIMM population rules for best memory loading and interleaving. Memory locations - CPU 0 and Memory locations - CPU 1 specify the DIMM location rules for various memory configurations.

Table 129. Memory locations - CPU 0

		Channel A		Channel B		Channel D		Channel C	
Tier	Total Memory	0	1	2	3	4	5	6	7
DLH Expanded	384 GB	32 GB	16 GB	32 GB	16 GB	16 GB	32 GB	16 GB	32 GB
DLH	192 GB	16 GB	N/A	16 GB	N/A	N/A	32 GB	N/A	32 GB
DLH Extended Retention/DD Cloud Tier	384 GB	32 GB	16 GB	32 GB	16 GB	16 GB	32 GB	16 GB	32 GB

Table 130. Memory locations - CPU 1

		Channel A		Channel B		Channel D		Channel C	
Tier	Total Memory	8	9	10	11	12	13	14	15

Table 130. Memory locations - CPU 1 (continued)

DLH Expanded	384 GB	32 GB	16 GB	32 GB	16 GB	16 GB	32 GB	16 GB	32 GB
DLH	192 GB	32 GB	N/A	32 GB	N/A	N/A	16 GB	N/A	16 GB
DLH Extended Retention/DD Cloud Tier	384 GB	32 GB	16 GB	32 GB	16 GB	16 GB	32 GB	16 GB	32 GB

DD9300 and ES30 shelf guidelines

The system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your system as listed in the following table below.
- Use the Installation and Setup Guide for your system to minimize the chance of a cabling mistake.
- A system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.
- DD6800 systems support ES30 SATA shelves after controller upgrades from older models.
- ES30 SATA shelves must be on their own chain.

Table 131. DD9300 and ES30 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	ES30 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB) [1]	Max RAW external capacity (TB) [2]
DD9300	192	2x4	SAS 30, 45, 60; SATA 15, 30, 45	7 [3]	4	384	480
DD9300 w/ Expanded Capacity [4]	384	2x4	SAS 30, 45, 60; SATA 15, 30, 45	7 [3]	4	720	900
DD9300 w/ Expanded Capacity or w/ HA [4]	384	2x4	SAS 30, 45, 60	7 [3]	4	720	900
DD9300 w/ ER	384	2x4	SAS 30, 45, 60; SATA 15, 30, 45	7 [3]	4	1440	1800
DD9300 Expanded Capacity w/ Cloud Tier	384	2x4	SAS 30, 45, 60; SATA 15, 30, 45	7 [3]	4	720 (max), additional 192 SAS dedicated to Cloud Tier	900 (max), additional 240 SAS dedicated to Cloud Tier
DD9300 w/ Expanded Capacity or w/ HA and Cloud Tier [4]	384	2x4	SAS 30, 45, 60	7 [3]	4	720 (max), additional 192 SAS dedicated to Cloud Tier	900 (max), additional 240 SAS dedicated to Cloud Tier

1. This figure only counts drives that have user data in the shelves.

2. The raw capacity of an ES30 is 125% of the available capacity.

3. Recommended configurations start at four shelves per set and expand beyond that as required. For HA configurations, the counts as a shelf.

4. DDOS 6.x and greater and SSD shelf configuration

Types of cabinets and power connections

The ES30 chassis is installed in two types of racks: 40U-C (existing racks) and the 40U-P (newer racks). The racks use one phase or 3-phase power connections.

3-Phase power connections for 40U-P (current racks)

Some environments use 3-phase power for 40U-P racks that are used for several systems. In those situations, it is desirable to balance the current draw across all three phases. The recommended 3-phase power cabling attempts to do that, but an optimal configuration depends on the specific installation.

Cabling shelves

NOTE:

- Before cabling the shelves, physically install all shelves in the racks. Refer to the rail kit installation instructions included with the ES30 shelf for rack mounting.
- The documentation refers to two SAS HBAs. If only one HBA is allowed in a system, then use another port as defined later for that specific system.
- On an HA system, add cables from the second node to open ports at the end of the sets. The ports on the second node must connect to the same sets as the corresponding ports on the first node.

Ports on the system's SAS HBA cards connect directly to a shelf controller's host port. For redundancy, you need to create dual paths by using a port on one SAS HBA card to connect to one shelf controller in each shelf set, and a port on another SAS HBA card to connect to another shelf controller in the same shelf set. With dual paths, if one SAS HBA card fails, the shelf is still operational. However, in the unlikely event any single shelf becomes completely disconnected from power or SAS cables and becomes disconnected from a previously operational shelf, the file system goes down and the shelf is not operational. This is considered a double failure.

There are two kinds of configurations: one shelf in a set or multiple shelves in a set.

DD6300, DD6800, and DD9300 shelf configurations

There are a few rules that must be followed when adding a mixture of DS60 and other shelf types to your system.

CAUTION: **If a system does not follow ALL of these rules it is not a legitimate configuration.**

Prerequisites:

- You cannot exceed the maximum amount of raw capacity displayed in the cabling table for each system.
- You cannot exceed the maximum number of shelves displayed in the cabling table for each system.
- There are no specific placement or cabling requirements for SSD shelves, or the metadata shelves for Cloud Tier configurations. These shelves can be installed and cabled the same way as standard ES30 shelves.

Table 132. Minimum and maximum configurations

System	Appliance	Minimum appliance shelf count*	Max appliance shelf count
	48 TB usable	0	1
w/ Expansion	144 TB usable	1	5
	144 TB usable	2	28
w/ Expansion	288 TB usable	2	28
w/ High Availability (HA)	288 TB usable	2	28
w/ Extended Retention (ER)	576 TB usable	2	28
w/ Cloud Tier	288 TB usable (96 TB for Cloud Tier)	2	28

Table 132. Minimum and maximum configurations (continued)

System	Appliance	Minimum appliance shelf count*	Max appliance shelf count
w/ HA and Cloud Tier	288 TB usable (96 TB for Cloud Tier)	2	28
	384 TB usable	3	28
w/ Expansion	720 TB usable	3	28
w/ HA	720 TB usable	3	28
w/ ER	1440 TB useble	7	28
w/ Cloud Tier	720 TB usable (192 TB for Cloud Tier)	7	28
w/ HA and Cloud Tier	720 TB usable (192 TB for Cloud Tier)	7	28

* The minimum appliance shelf count does not include shelves for Cloud Tier.

DD9300 and DS60 shelf guidelines

The system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your system as listed in the following table.
- For redundancy, the two connections from a system to a set of shelves must use ports on different SAS I/O modules.
- Use the Installation and Setup Guide for your system to minimize the chance of a cabling mistake.
- A system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.
- ES30 SATA shelves must be on their own chain.
- If ES30 SAS shelves are on the same chain as a DS60, the maximum number of shelves on that chain is 5.

Table 133. DD9300 and DS60 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	DS60 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB)[1]	Max RAW external capacity (TB)
DD9300 [2, 3, 4]	192[5]	2x4	SAS 45, 60	3	4	384	480
DD9300 w/ Expanded Capacity [2, 3, 6]	384	2x4	SAS 45, 60	3	4	720	900
DD9300 w/ Expanded Capacity and w/ HA [2, 3]	384	2x4	SAS 45, 60	3	4	720	900
DD9300 w/ Expanded Capacity and w/ ER [2, 3, 7]	384	2x4	SAS 45, 60	3	4	1440	1800
DD9300 w/ Expanded Capacity and w/ Cloud Tier [3, 6]	384	2x4	SAS 45, 60	3	4	720 + 192 for Cloud Tier	900 + 240 for Cloud Tier
DD9300 w/ Expanded Capacity and w/ HA and Cloud Tier [3, 6]	384	2x4	SAS 45, 60	3	4	720 + 192 for Cloud Tier	900 + 240 for Cloud Tier

NOTE: An entry of 45 corresponds to DS60-3 models and an entry of 60 corresponds to DS60-4 models.

1. This column only counts drives that have user data in the shelves. For example, a DS60 4-240 has 192TB.

2. With DD OS 6.x and greater & SSD.

3. Only available with DD OS 6.x and greater.

4. DD9300 base support 2.5 DS60-4 180 x 2 plus DS60-2 90, if a half-filled DS60 is necessary.

5. While it is 192GB, it is a different memory DIMM configuration compared to DD6300 's 192GB.

6. DD9300 Expanded supports five DS60 maximum.

7. There is no support for HA with SATA drives.

8. The maximum shelf count for any specific drive/shelf size might be less than the product of max shelves x max shelves per set.

3-phase power connections for 40U-P (current racks)

Some environments use 3-phase power for 40U-P racks used for several systems. In those situations it is desirable to balance the current draw across all 3 phases. The recommended 3-phase power cabling attempts to do that, but an optimal configuration is dependent on the specific installation.

shelf configurations

There are a few rules that must be followed when adding a mixture of DS60 and other shelf types to your system.

CAUTION: **If a system does not follow all these rules, it is not a legitimate configuration.**

Prerequisites:

- You cannot exceed the maximum amount of raw capacity displayed in cabling table for each system.
- You cannot exceed the maximum number of shelves displayed in cabling table for each system.
- You cannot connect more than three DS60 shelves in a single set.

Table 134. Minimum configurations

System	Appliance maximum	Minimum appliance DS60 shelf count
	144 TB	0
	144 TB	2
w/ High Availability (HA)	288 TB	2 (plus 1 FS15 for SSD cache)
w/ Extended Retention (ER)	576 TB	2
w/ Cloud Tier	384 TB (96 TB for Cloud Tier)	2 (plus 2 ES30s for Cloud Tier)
w/ HA and Cloud Tier	384 TB (96 TB for Cloud Tier)	2 (plus 1 FS15 for SSD cache, and 2 ES30s for Cloud Tier)
	384 TB	3
w/ HA	720 TB	3 (plus 1 FS15 for SSD cache)
w/ ER	1440 TB	3
w/ Cloud Tier	912 TB (192 TB for Cloud Tier)	3 (plus 4 ES30s or 1 DS60 for Cloud Tier)
w/ HA and Cloud Tier	912 TB (192 TB for Cloud Tier)	4 (plus 1 FS15 for SSD cache, and 4 ES30s or 1 DS60 for Cloud Tier)

1. DS60 will only be partially filled.

- A Cloud Tier system shares the ERSO cabling configuration; however, Cloud Tier has a lower maximum.
- It is recommended that the shelf with the greater number of drives should always be placed in the bottom position.
- only supports one DS60.
- only has one SAS SLIC and all DS60 connections are made to that single SAS SLIC.

- only has one SAS SLIC and all DS80 connections are made to that single SAS SLIC.

11

DD9400

This chapter contains the following topics:

Topics:

- DD9400 system features
- DD9400 system specifications
- DD9400 storage capacity and configurations
- DD9400 front panel
- DD9400 SSD usage and configurations
- Rear panel
- PCIe HBAs
- DD9400 DIMM configurations
- DD6900, DD9400, and DD9900 storage shelves configurations and capacities

DD9400 system features

Table 135. DD9400 system features

Features		Single Node	HA
Processor		2 x Intel Xeon 5218, 16C, 2.3GHz, 125W	
Kernel		4.4	
Memory Configurations	Total	576 GB	
	DIMMs	12 x 16 GB + 12 x 32 GB	
HDD Drive Size		8 TB (3 TB and 4 TB also supported)	
Supported Capacity	Active Tier	192 <-> 768 TBu	
	Cloud Tier	1536 TBu	
Disk Groups	Active Tier	4 <-> 10 (8 TB), 4 <-> 16 (4 TB), 4 <-> 21 (3 TB)	
	Cloud Tier (4 TB)	4	
SSDs for DD OS in 2.5" bays in head		4, 1.92 TB, 1 WPD	
Stream Count		800 Wr, 220 Rd	
Cache SSDs in 2.5"	2.5%	5 (internal) 3.84 TB	5 (External FS25) 3.84 TB
Cache SSD shelf	FS25	0	1
HA Private Interconnect		N/A	(2) 10G Base-T ports (NDC)
16 GB NVRAM		1	
HW Accelerator	100 Quick Assist Technology (QAT) 8970	1	
Internal SAS	HBA330 12 Gbps SAS controller	1	
External SAS	PMC Quad Port 12 Gbps SAS	2 default, 3 supported	

Table 135. DD9400 system features (continued)

Features		Single Node	HA
SAS String Depth (max)	ES30/ES40	7	
	DS60	3	
Host interface HBAs	2-port QL41000 25 GbE-SFP28	4 maximum	
	4-port QL41164 10 GbE-SFP+	4 maximum	
	4-port QL41164 10GBASE-T	4 maximum	
	4-port QLE2694 16 Gb FC	3 maximum	
Network Daughter Card option (system will have one of the two options)	4-port QL41000 10 GbE-SP+ FasLinQ	1	
	4-port QL41164 10GBASE-T	1	

DD9400 system specifications

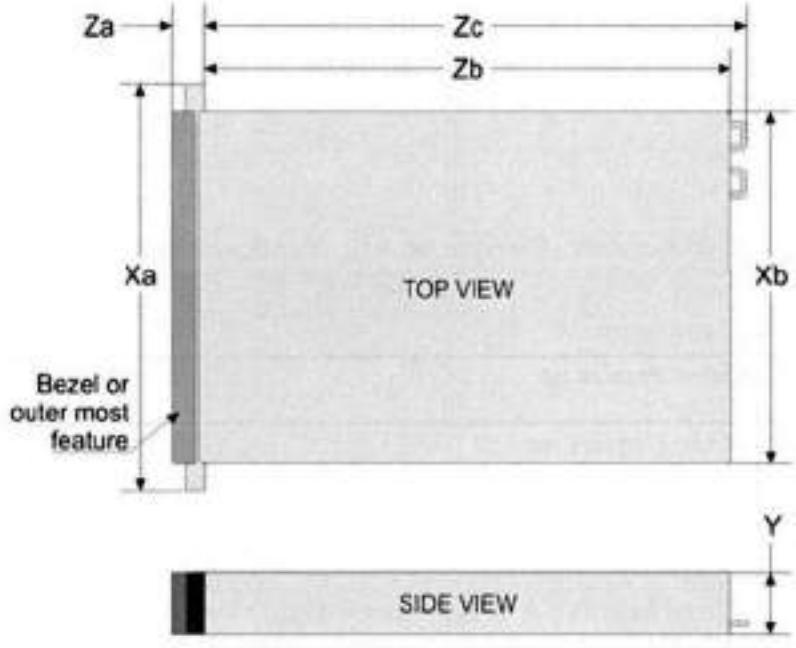


Figure 121. System dimensions

Table 136. DD9400 system specifications

Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb	Zc
482.0 mm (18.98 inches)	434.0 mm (17.09 inches)	86.8 mm (3.42 inches)	35.84 mm (1.41 inches)	22.0 mm (0.87 inches)	678.8 mm (26.72 inches)	715.5 mm (28.17 inches)

A DD9400 system weighs up to 63.05 lbs (28.6 kg).

Table 137. System operating environment

Operating Temperature	50° to 95° F (10° to 35° C), derate 1.1° C per 1000 feet, above 7500 feet up to 10,000 feet (32.25° C at 10,000)
Operating Humidity	20% to 80%, non-condensing
Non-operating Temperature	-40° to +149° F (-40° to +65° C)
Operating Acoustic Noise	L_{wad} sound power, 7.5 Bels

DD9400 storage capacity and configurations

The following table provides storage capacity and configuration information for the DD9400 system.

Table 138. DD9400 storage capacity and configurations

Tier	CPU-SP SKU	Memory	Front 2.5" SSDs	Max. Useable Capacity	Cloud Tier Metadata
DD9400 Active Tier	16 core, 125 W 5218	576 GB (12 x 16 GB) + (12 x 32 GB)	5 (2.5%)	768TBu	N/A
DD9400 with Cloud Tier [1]	16 core, 125 W 5218	576 GB (12 x 16 GB) + (12 x 32 GB)	5 (2.5%)	1248TBu	240 TB raw/192 TB usable

[1]Cloud Tier can be added to a DD9400 and is enabled by a license and disk packs for the Cloud Tier metadata.

The Memory column lists the total memory that is required and the number and type of the DIMMs used. All memory DIMMs are DDR4 RDIMMs at the highest supported speed of 2666MT/s.

High Availability

DD9400 supports Active-Passive High Availability (A-P HA or just A-P). The following table summarizes the hardware changes to support A-P HA:

Table 139. HA configuration requirements

Hardware Change to support HA	Active-Passive HA
Additional memory	No extra memory required.
HA private interconnect	Cluster Interconnect : A-P requires the use of two ports from the on-board quad-port 10 GbE Network Daughter Card.
NVRAM	A-P requires a single 16 GB NVRAM card (same as non-HA).
SAS Connectivity	Both nodes of an A-P HA pair require redundant SAS connectivity to the storage array. (Note: a single node system also has redundant connectivity to the storage array.)
SSD Requirements	SSDs are contained within FS25 and are available from both nodes.

HA Network Interconnect

The HA Network Interconnect, required for HA configurations, is a dedicated 10 GbE connection between the two nodes of an HA pair. The interconnect is used to write data (and metadata) from the active node's NVRAM to the passive node's NVRAM.

Two 10GbE links are used to meet the bandwidth requirements for the private interconnect. Traffic across the private interconnect has roughly the same bandwidth as is written to the NVRAM card. The dual 10-GbE links can move about 2 GB/s in each direction.

HA SAS Interconnect

HA configurations require that the SSDs' cache drives be shared between both nodes and have redundant SAS connections to all shelves.

DD9400 front panel

Figure 122. DD9400 front panel

Table 140. Front panel features

Item	Ports, panels, and slots	Description
1	Left control panel	Contains system health and system ID, status LED, and optional iDRAC Quick Sync 2 (wireless).
2	Drive slots	Enable you to install drives that are supported on your system.
3	Right control panel	Contains the power button, VGA port, iDRAC Direct micro USB port, and two USB 2.0 ports.
4	Information tag	The Information tag is a slide-out label panel that contains system information such as Service Tag, NIC, MAC address, and so on. If you have opted for the secure default access to iDRAC, the Information tag also contains the iDRAC secure default password.

Table 141. Front LEDs

Name	Color	Purpose
Control Panel Status LED	Blue/Amber	Status: • Healthy: Solid Blue • Fault: Blink Amber • Sys ID: Blink Blue
System Power Button/LED	Green	Indication that the system has power.
Drive activity LEDs	Green	Lit green when the drive is powered. Blinks during drive activity.
Drive service LEDs	Green	Lit solid amber when a disk drive needs service.

Front LEDs

Figure 123. Front left control panel status LEDs

NOTE: The indicators display solid amber if any error occurs.

Table 142. System health and system ID indicator codes

System health and ID indicator code	
Solid blue	Indicates that the system is turned on, system is healthy, and system ID mode is not active. Press the system health and system ID button to switch to system ID mode.
Blinking blue	Indicates that the system ID mode is active. Press the system health and system ID button to switch to system health mode.
Solid amber	Indicates that the system is in fail-safe mode.
Blinking amber	Indicates that the system is experiencing a fault. Check the System event log or the LCD panel, if available on the bezel, for specific error messages.

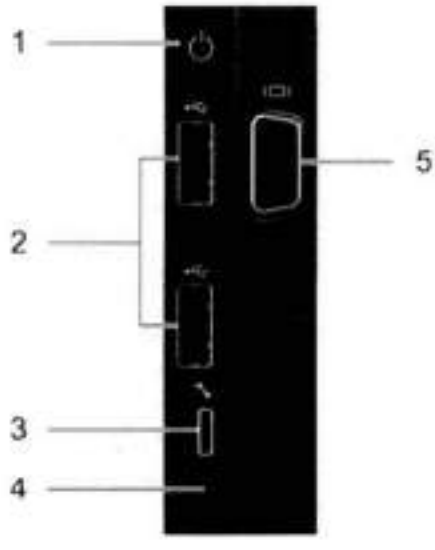


Figure 124. Front right control panel power button LEDs

Table 143. Right control panel features

Item	Indicator, button, or connector	Description
1	Power button	Indicates if the system is turned on or off. Press the power button to manually turn on or off the system. **NOTE:** Press the power button to gracefully shut down an ACPI-compliant operating system.
2	USB port (2)	The USB ports are 4-pin, 2.0-compliant. These ports enable you to connect USB devices to the system.
3	iDRAC Direct port	The iDRAC Direct port is micro USB 2.0-compliant. This port enables you to access the iDRAC Direct features.
4	iDRAC Direct LED	The iDRAC Direct LED indicator lights up to indicate that the iDRAC Direct port is connected.
5	VGA port	Enables you to connect a display device to the system.

Table 144. iDRAC Direct LED indicator codes

iDRAC Direct LED indicator code	Condition
Solid green for two seconds	Indicates that the laptop or tablet is connected.
Flashing green (on for two seconds and off for two seconds)	Indicates that the laptop or tablet that is connected is recognized.
Turns off	Indicates that the laptop or tablet is unplugged.

Figure 125. Drive LEDs

The front contains 25 2.5" disk drive slots that can be populated with SSDs. Each SSD is housed in a drive carrier that contains two LEDs at the bottom of the carrier. The carrier's left blue LED is lit whenever an SSD is present in the slot, and it blinks when I/O activity is occurring on the disk. The right amber LED is usually off and lights amber to indicate that the disk is faulted and must be serviced.

DD9400 SSD usage and configurations

DD9400 system uses a 16 x 2.5" drive slot midplane. In addition to the operating system drives, it allows up to 12 SSD drives for metadata cache implementation.

SSD configurations

The SSD slots on the front of the enclosure are shown below. The system come from the factory with SSDs populated in the enclosure.

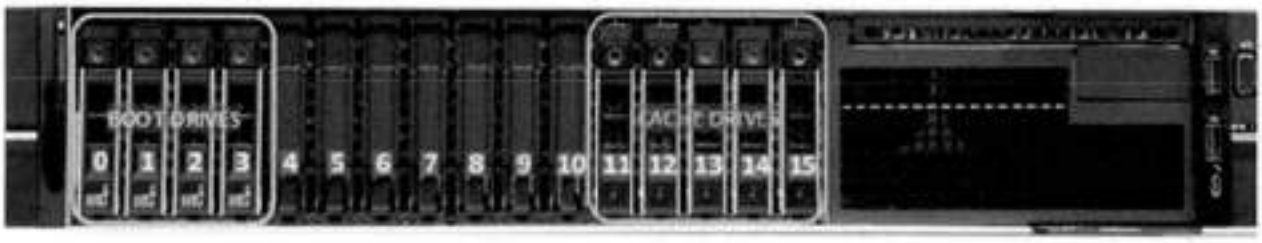


Figure 126. DD9400 SSD slot assignment (single node configuration)

DD9400 supports 2.5% SSD option out of factory. Based on 3.84 TB SSD capacity, the required number of SSDs for each DD9400 configuration is provided in the following table.

Table 145. DD9400 SSD configurations

Configuration	Single node	HA
Cache SSDs	5 (internal) 3.84 TB	5 (External FS25) 3.84 TB

The cache SSDs are installed right to left starting from slot 15 down.

NOTE: For DD9400 HA configuration, the head unit will only have the four boot drives. It will not have the cache drives in the head unit as shown in the above figure because the cache drives are in the FS25 data shelf.

SSD boot drives

Other SAS SSDs are used to boot the DD OS operating system. Boot disks and/or external disk shelves are used to log system information. Boot disks are installed from the other end of the front 2.5" disk slots to physically differentiate the cache SSDs.

Table 146. SSD boot drives

# of boot disks	Installed in slots
Four 1.92TB SSDs	0,1,2,3

Rear panel

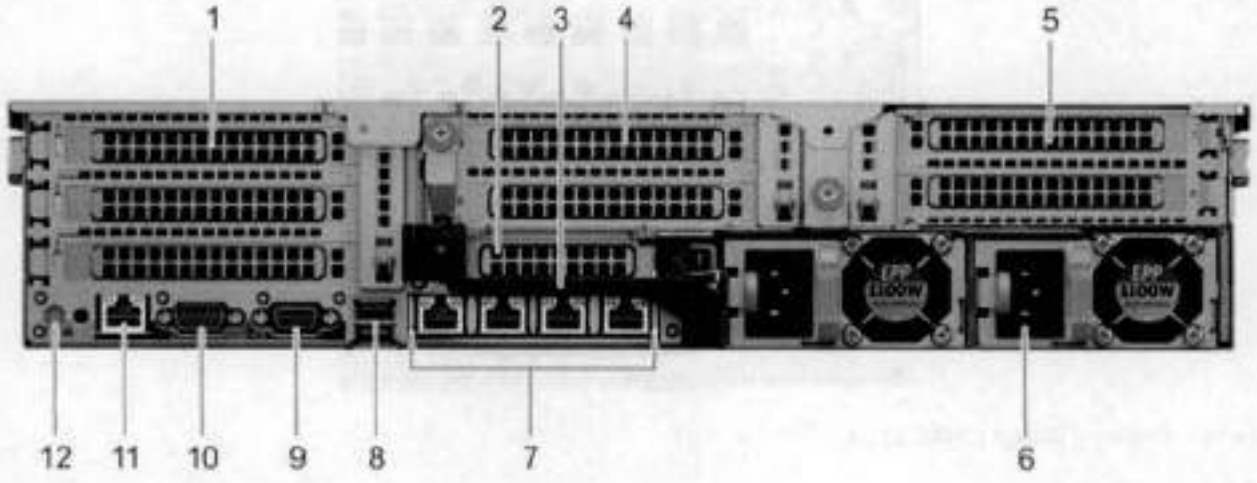


Figure 127. System rear panel

Item	Panels, ports, and slots	Description
1	Full-height PCIe expansion card slot (3)	The PCIe expansion card slot (riser 1) connects up to three full-height PCIe expansion cards to the system.
2	Half-height PCIe expansion card slot	The PCIe expansion card slot (riser 2) connects one half-height PCIe expansion cards to the system.
3	Rear handle	The rear handle can be removed to enable any external cabling of PCIe cards that are installed in the PCIe expansion card slot 6.
4	Full-height PCIe expansion card slot (2)	The PCIe expansion card slot (riser 2) connects up to two full-height PCIe expansion cards to the system.
5	Full-height PCIe expansion card slot (2)	The PCIe expansion card slot (riser 3) connects up to two full-height PCIe expansion cards to the system.
6	Power supply unit (2)	Supports two AC power supply units (PSUs)
7	NIC ports	The NIC ports that are integrated on the network daughter card (NDC) provide network connectivity.
8	USB port (2)	The USB ports are 9-pin and 3.0-compliant. These ports enable you to connect USB devices to the system.
9	VGA port	Enables you to connect a display device to the system.
10	Serial port	Enables you to connect a serial device to the system.
11	iDRAC9 dedicated port	Enables you to remotely access iDRAC.
12	System identification button	The System Identification (ID) button is available on the front and back of the systems. Press the button to identify a system in a rack by turning on the system ID button. You can also use the system ID button to reset iDRAC and to access BIOS using the step through mode.

Rear LEDs

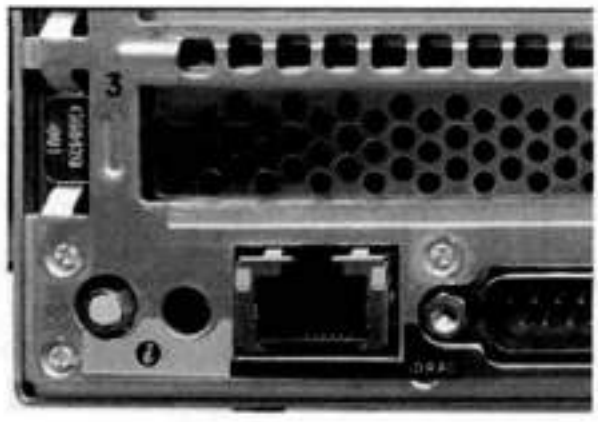


Figure 128. Onboard ID and iDRAC LEDs

1. iDRAC management port:
   a. The green link LED on the left is lit whenever there is link at 1000BaseT and 100BaseT speeds. The link LED is off when the link speed is 10BaseT or there is no link.
   b. The green link LED on the right blinks whenever there is traffic on the port.
2. System identification LED: This blue LED can be turned on by software to visually identify the system.

PSU FRU LEDs

There are two power supplies, one in the upper left of the rear chassis and one on the bottom right. Each power supply has three LEDs: AC good, DC good, and Service. The top PSU is "right-side up" and the bottom PSU is "upside down."

Table 147. PSU FRU LEDs

Name	Color	Definition
AC Good	Green	AC input is as expected.
DC Good	Green	DC output is as expected.
Service	Amber	PSU has a fault condition and a must be replaced.

PCIe HBAs

A slot in the chassis that does not contain an HBA must have a filler panel installed in the empty slots. This is required for EMI compliance.

This system supports nine I/O modules slots, seven of which are 8-lane PCIe Gen3, and two are 16-lane PCIe Gen3. Several networking, NVRAM, SAS, and Fibre Channel I/O modules are supported.

Slot assignment

The following table lists the DD9400 configuration slot assignments:

Table 148. DD9400 slot assignments

Description	Slot
QLogic, 41164 4 Port, 10GbE SFP+ PCIe, Full Height	5, 8, 1

Table 148. DD9400 slot assignments (continued)

Description	Slot
QLogic, 41164 4 Port, 10GBASE-T PCIe, Full Height	5, 8, 1
QLogic, 41164 4 Port, 10GBASE-T PCIe, Low Profile	6
QLogic, 41262 2 Port, 25Gb SFP28 PCIe, Full Height	5, 8, 1
QLogic, 41262 2 Port, 25Gb SFP28 PCIe, Low Profile	6
HBA330 SAS Controller, 12Gbps Mini card	mini/mono
QAT,INTEL,8970,FH, Avnet p/n 1QA89701G1P5	4
PM8072,SAS12.4P,FH, MicroSemi 2295200-R	3, 7, 5
FC16,QLE2694-DEL-BK,TRG,QP,FH	5, 8, 1
16GB NVRAM,FH	2

Host Interface (x16) is 2-port 100 Gb QSFP+ Ethernet.

Host Interface (x8) are:

- 2-port 25 Gb SFP28 Ethernet
- 4-port 10 Gb SFP+ Ethernet
- 4-port 10GBaseT Ethernet
- 4-port 16 Gb Fibre Channel

External SAS is 4-port 12 Gb SAS card and is required for external storage for HA and Single Node configurations.

NVRAM is the 16GB NVRAM.

Internal SAS Mezzanine is 2-port 12 Gb Mini-SAS HD SAS controller mezzanine.

Host Network Interface Mezzanine is either:

- 4-port 10GBaseSR SFP+ Ethernet mezzanine
- 4-port 10GBaseT RJ45 Ethernet mezzanine

I/O population rules

The following figures show the I/O module slot numbers.

The slot labeled N is the network daughter card, which contains ports ethMa, ethMb, ethMc, and ethMd.

The physical interface name format for the other I/O module slots is ethXy, where X is the slot number and y is an alphanumeric character. For example, eth0a.

For most horizontal I/O module NIC interfaces, the port numbering goes from left to right, with ethXa on the left. The horizontal I/O module slots on the left-in slots 1-3 are inverted. The port numbering on these I/O modules in these slots goes from right to left, with ethXa on the right.

The management port ethMa is the first port set up by the Configuration Wizard. It is marked with a red rectangle in the figure below.

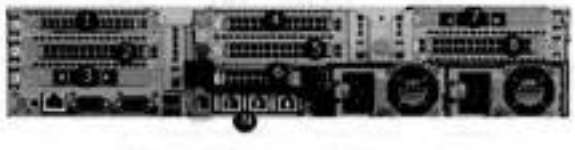


Figure 129. Slot numbering

The general population rules can be summarized as:

1. Populate a given I/O in the available slots listed.
2. Select the first available slot in the group.
3. Follow the steps for each I/O in the order specified.

4. Slots 4 and 8 should be reserved for x16 cards unless there are no available x8 slots.

NOTE: Installing HBAs requires opening the system and installing the HBA into the riser.

Riser#	Slots (from top to bottom)
1	1, 2, 3
2	4, 5, 6, N
3	7, 8

Gen3 PCIe

Slots support Gen3 PCIe.

I/O module servicing

All I/O modules are user serviceable and may be replaced when the system is powered off. On-line service of I/O modules is not support. A module that is hot-inserted into the system will remain powered off and will not be powered on until the next reboot of the system. A module that is hot-removed causes an operating system to immediately reboot.

DD9400 DIMM configurations

The SP Module contains two Intel SP processors each with an integrated memory controller that supports six channels of DDR4 memory. The CPU allows two DIMM slots per channel, so the SP Module supports 24 DIMM slots.

Each DDR4 DIMM is connected to the system board through an industry standard 288-pin DDR4 DIMM connector. This system uses registered DIMMs with Dell EMC ControlCenter at 72 bits wide (64-bits data + 8-bits Dell EMC ControlCenter) up to a maximum of 2666MT/s speed.

Table 149. Memory configurations

Tier	Total Memory	Memory DIMM Configuration
DD9400 Active Tier	576 GB	12 x 32 GB + 12 x 16 GB
DD9400 Cloud Tier	576 GB	12 x 32 GB + 12 x 16 GB

Memory locations

To ensure maximum memory performance, there are memory DIMM population rules so that the memory loading and interleaving are optimal. The following table specifies the DIMM location rules. Each DIMM location contains a 16GB DIMM or a 32GB DIMM.

Table 150. DD9400 DIMM configuration CPU 1

Total (GB)	Channel C		Channel B		Channel A		Channel D		Channel E		Channel F	
	A6	A12	A5	A11	A4	A10	A7	A1	A8	A2	A9	A3
288 GB	32 GB	16 GB	32 GB	16 GB	32 GB	16 GB	16 GB	32 GB	16 GB	32 GB	16 GB	32 GB

Table 151. DD9400 DIMM configuration CPU 2

Total (GB)	Channel C		Channel B		Channel A		Channel D		Channel E		Channel F	
	B6	B12	B5	B11	B4	B10	B7	B1	B8	B2	B9	B3
288 GB	32 GB	16 GB	32 GB	16 GB	32 GB	16 GB	16 GB	32 GB	16 GB	32 GB	16 GB	32 GB

DD6900, DD9400, and DD9900 storage shelves configurations and capacities

DD6900, DD9400, and DD9900 do not store data on internal disk drives and rely on external disk array shelves to provide storage. DS60 disk shelves and ES40 shelves are connected to systems using 12 Gb Mini-SAS HD ports, which are implemented on the SAS HBAs.

The systems also support external metadata storage (cache) shelf FS25. External cache shelf only hosts DD OS depended metadata for performance acceleration.

The ES40 SAS shelf contains 15 drives, which includes 12 drives of usable storage, two parity drives, and one hot spare.

The DS60 shelf contains 60 drives. Drives are configured in four groups of 15 drives. Each group contains two parity drives and one hot spare, so each group provides 12 drives of usable storage. A fully configured DS60 shelf provides 48 drives of usable storage.

Table 152. Shelves shipped from factory, in rack

DD6900	DD9400	DD9900
4 TB ES40	8 TB DS60	8 TB DS60

Table 153. Shelves shipped from factory, boxed

DD6900	DD9400	DD9900
4 TB ES40	8 TB ES40	8 TB ES40
4 TB DS60	8 TB DS60	8 TB DS60

Table 154. Additional shelves supported

DD6900	DD9400	DD9900
4 TB SAS ES30/DS60	4 TB SAS ES30/DS60	4 TB SAS ES30/DS60
3 TB SAS ES30/DS60	3 TB SAS ES30/DS60	3 TB SAS ES30/DS60

NOTE: 3 TB shelves are only support on controller upgrades and not on fresh installs.

Table 155. Shelf usable capacities

Hard drive size (TB)	Shelf	Useable TB
4	ES40	48
4	DS60	192
8	DS60	384

The following table lists the maximum number of shelves per chain:

Table 156. Supported shelf count per chain

Shelf type	Max # from factory	Max # per chain
SAS ES30/ES40	4	7
DS60	2	3
DS60 + ES30/ES40	n/a	5
F25	1	1

The connector type for ES30 is Mini-SAS. Special cables may be necessary when combining ES30 and ES40 shelves on the same chain (enabled but not recommended).

DD9400 and DD9900 system capacities are optimized for use with DS60 shelves containing 8 TB drives. DS60 shelves can be populated with one to four packs of fifteen 8 TB, or 4 TB drives. Different 4 TB and 8 TB capacity disk packs may be mixed

within a single DS60 shelf. ES40 SAS shelves and DS60 shelves of mixed capacities may be attached so long as the maximum storage capacity of the system is not exceeded.

12

DD9500

This chapter contains the following topics:

Topics:

- System features
- System specifications
- DD9500 storage capacity
- Front panel
- Rear panel
- I/O module slot assignments
- Internal System Components
- DD9500 and ES30 shelf guidelines
- DD9500 and DS60 shelf guidelines

System features

Table 157. DD9500 system features

Feature		DD9500 (Base configuration)	DD9500 (Expanded configuration)
Rack height		4U, supported in four-post racks only	4U, supported in four-post racks only
Rack mounting		Rack mount kit included with each system. Adjustable between 24 - 36 in. (60.9–76.2 cm).	Rack mount kit included with each system. Adjustable between 24 - 36 in. (60.9–76.2 cm).
Power		4 hot-swappable power units, 2 pairs of 1 +1 redundant	4 hot-swappable power units, 2 pairs of 1 +1 redundant
Voltage		200–240 V~. Frequency: 50 Hz to 60 Hz.	200–240 V~. Frequency: 50 Hz to 60 Hz.
Processor		4 Intel EX processors	4 Intel EX processors.
NVRAM		One 8-GB NVRAM module for data integrity during a power outage	One 8-GB NVRAM module for data integrity during a power outage
Fans		8 hot-swappable fans, redundant	8 hot-swappable fans, redundant
Memory		32 x 8 GB DIMM (256 GB)	32 x 8 GB DIMM + 16 x 16 GB DIMM (512 GB)
Internal drives		4 x 400 GB (base 10) hot-swappable solid state drives (SSD)	4 x 400 GB (base 10) hot-swappable solid state drives (SSD)
I/O module slots		11 I/O module (Fibre Channel, Ethernet, and SAS) slots. Replaceable I/O modules are not hot-swappable. See I/O module slot assignments	11 I/O module (Fibre Channel, Ethernet, and SAS) slots. Replaceable I/O modules are not hot-swappable. See I/O module slot assignments
Supported capacity	Non-extended retention	540 TB	1080 TB
	DD Cloud Tier	N/A	2160 TB[a]
	Extended retention	N/A	1080 TB[b]
High availability support		Yes	Yes
HA private interconnect		4 10 GbE optical ports	4 10 GbE optical ports
External SSD shelf		Optional 1 x 8 drive SSD shelf	Optional 1 x 15 drive SSD shelf

a. DD Cloud Tier requires five ES30 shelves fully populated with 4 TB drives to store DD Cloud Tier metadata.
b. Extended retention not available on HA configurations

System specifications

Table 158. DD9500/DD9800 system specifications

Model	Watts	BTU/hr	Power (VA)	Weight	Width	Depth	Height
DD9500/ DD9800	1887	6444	1981	117 lb / 53.2 kg	19 in / 48.3 cm	29.5 in / 74.9 cm	7 in / 17.8 cm

- Operating temperature: 50° to 95° F (10° to 35° C), derate 1.1° C per 1000 feet, above 7500 feet up to 10,000 feet
- Operating humidity: 20% to 80%, non-condensing
- Non-operating temperature: -40° to +149° F (-40° to +65° C)
- Operating acoustic noise: Sound power, LWAd, is 7.7 bels.

DD9500 storage capacity

The table lists the capacities of the systems. The internal indexes and other product components use variable amounts of storage, depending on the type of data and the sizes of files. If you send different datasets to otherwise identical systems, one system may, over time, have room for more or less actual backup data than another.

NOTE: The system commands compute and display amounts of disk space or data as decimal multiples of certain powers of two (2^{10}, 2^{20}, 2^{30}, and so forth). For example, 7 GiB of disk space = 7 x 2^{30} bytes = 7 x 1,073,741,824 bytes. The system sees this process as Base 2 calculation.

Table 159. DD9500 storage capacity

System/Installed Memory	Internal Disks	Raw Storage (Base 10)	Data Storage Space (Base 2 Calculation)	Data Storage Space (Base 10 Calculation)
DD9500 (3 SAS I/O modules) 256 GB	2.5 in.; 4 x 400 GB SATA SSD No User Data	540 TB (external)	392.9 TiB	432 TB
DD9500 (3 SAS I/O modules) 512 GB	2.5 in.; 4 x 400 GB SATA SSD No User Data	1,080 TB (external)	786.8 TiB	864 TB
DD9500 with DD Cloud Tier software (4 SAS I/O modules) 512 GB	2.5 in.; 4 x 400 GB SATA SSD No User Data	3,240 TB (external)	2360.4 TiB	2592 TB
DD9500 with Extended Retention (ER) software (4 SAS I/O modules) 512 GB	2.5 in.; 4 x 400 GB SATA SSD No User Data	2,160 TB (external)	1573.6 TiB	1728 TB

Table 160. DD9500 with ES30 SAS shelves

	DD9500	DD9500
Memory (GB)	256	512
SAS I/O modules x ports per module	3x4	3x4
ES30 support (TB)	SAS 30, 45, 60	SAS 30, 45, 60
Maximum shelves per set	5	5
Maximum number of sets	6	6

NOTE: ES30 SATA shelves are supported when upgrading from an older single node system, but are not supported with HA pairs or new installations.

Table 161. DD9500 with DS60 shelves

	DD9500	DD9500
Memory (GB)	256	512
SAS I/O modules x ports per module	3x4	3x4
DS60 support (TB)	SAS 45, 60	SAS 45, 60
Maximum shelves per set	4	4
Maximum number of sets	6	6

Front panel

The four solid state drives (SSDs), the storage processor (SP), and the fans are accessed from the front of the system. The SP must be pulled out to provide access to the DIMMs. The fans are accessed without pulling or removing the SP and they are hot-swappable. The photo shows the interfaces on the front of the system.

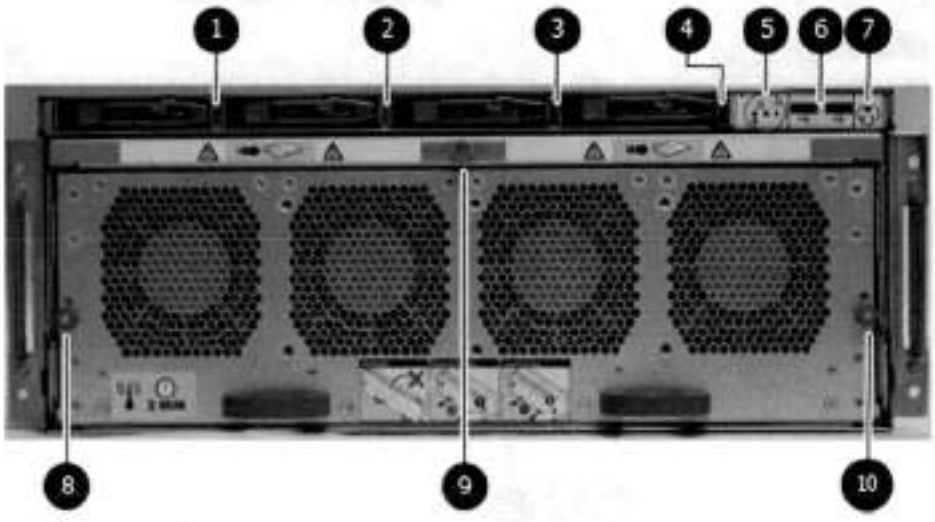


Figure 130. Front panel components

1. SSD slot 0
2. SSD slot 1
3. SSD slot 2
4. SSD slot 3
5. Front LEDs
6. USB ports
7. Power button
8. Fan tray thumbscrew (left)
9. SP module thumbscrew to secure the ejector handle
10. Fan tray thumbscrew (right)

Front LED indicators

On the front panel to the right of SSD #4 (in Slot 3) are 3 LEDs that show high level system status. The System Power LED glows blue to show the system is powered on.

NOTE: The system can have power (be plugged in) but the blue LEDs are off if the system is powered off.

The SP Service LED is normally off, but glows amber whenever the storage processor (SP) requires service. The Enclosure Service LED is normally off, but glows amber whenever the SP or other replaceable parts require service. The System Power and Enclosure Service LEDs are visible through the front bezel.

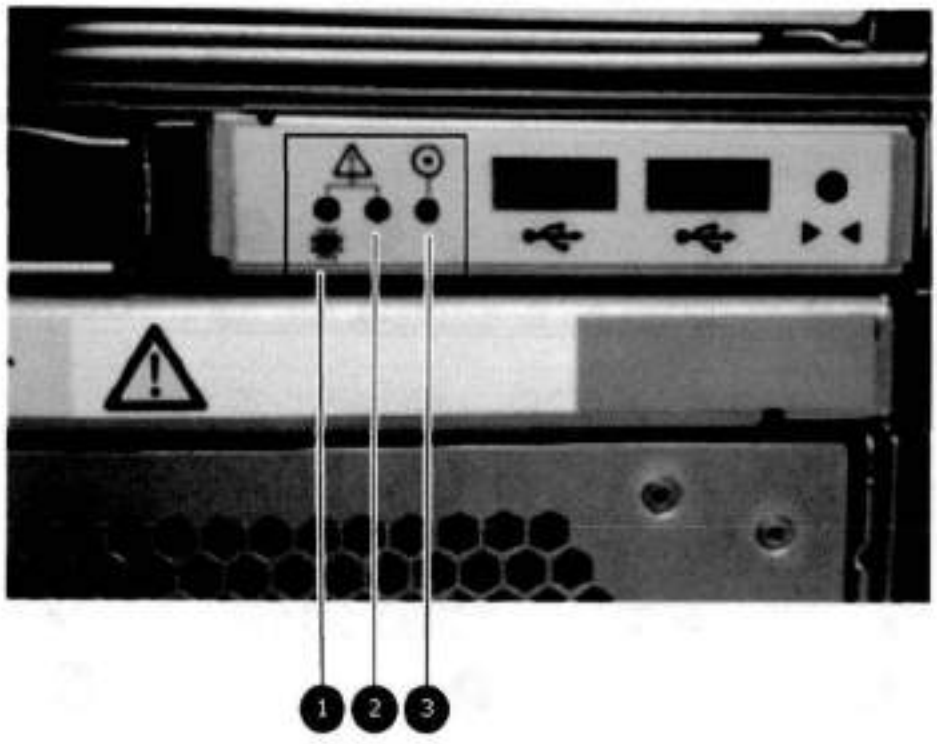


Figure 131. Service LEDs

1. SP service LED — Amber light indicates that the SP or one of its components needs service.
2. Enclosure Service LED — This is normally off, but amber light indicates that the enclosure or something within the enclosure— the fans, SP, I/O modules, management module etc—requires service.
3. System power LED — Blue light indicates system running

The power button shown in the picture is used when a system needs to be powered up after a shut down using the `system poweroff` command. Once power is restored the system power LED light turns blue.

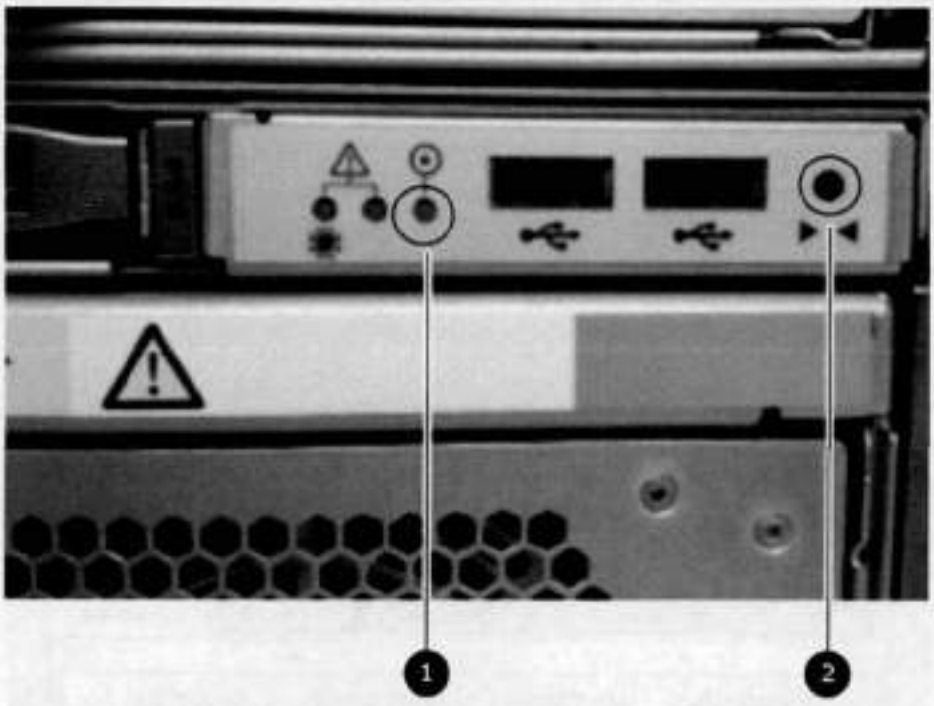


Figure 132. Power button

1. System power LED — Blue light indicates system running
2. Power button

The LEDs in the front are shown in the following figure.

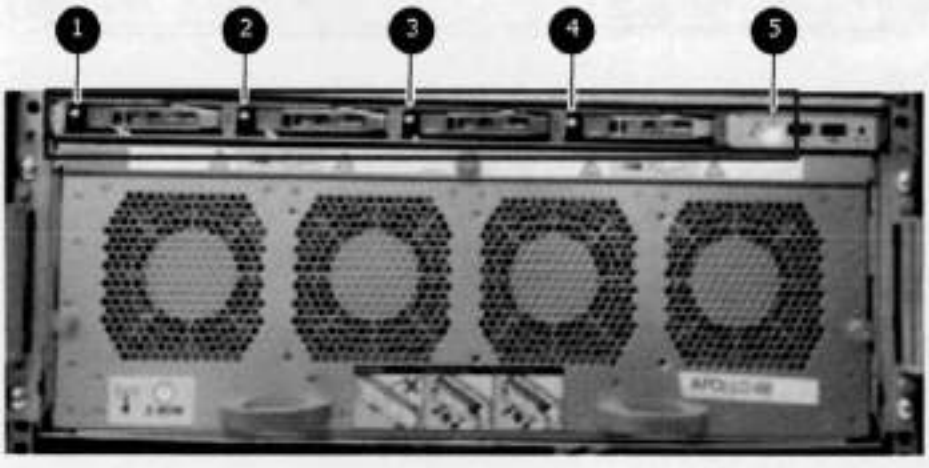


Figure 133. Front LEDs

1. SSD LED in slot 0
2. SSD LED in slot 1
3. SSD LED in slot 2
4. SSD LED in slot 3
5. System power LED — Blue light indicates system running

Table 162. Front panel LED status indicators

Part	Description or Location	State
System, SP fault	Exclamation point within a triangle	Dark indicates normal operation. Amber indicates failure.
System, chassis fault	Exclamation point within a triangle	Dark indicates normal operation. Amber indicates a fault condition.
SSD	Top LED	Solid blue, disk ready, blinks while busy.
SSD	Bottom LED	Dark indicates healthy. Solid amber indicates disk fail.

Solid-state drives

A system contains 4 hot-swappable 2.5 in. 400 GB solid-state drives (SSD) located in the front. There are four drive bays numbered 0–3 from left to right. A dual drive failure allows the system to operate without disruption.

Each drive has a blue colored power LED and an amber fault LED.

Figure 134. SSD drives

1. Slot 0
2. Slot 1
3. Slot 2
4. Slot 3

Rear panel

In the rear of the system, the top section contains the 4 power supply units. In the middle of the section, on the left, is serial number tag location. To the right of the serial number tag location is the management module. The lower section contains the NVRAM and the I/O modules numbered 0 through 11 from left to right. The photo shows the hardware features and interfaces on the rear of the system.

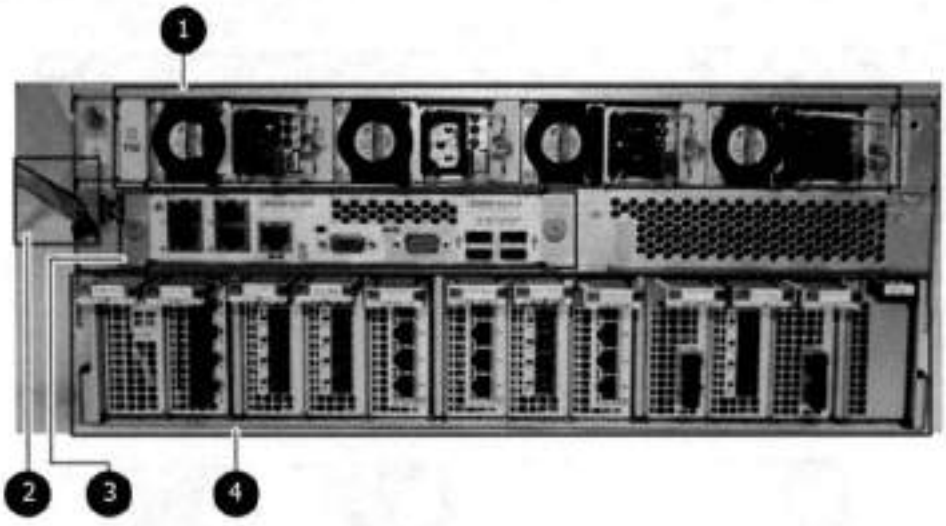


Figure 135. Features on rear of chassis

1. Power supply units
2. Serial number tag
3. Management module
4. NVRAM and I/O modules (slots 0-11)

The figure shows the location of the serial number tag on the left of the management module.

Figure 136. Serial number tag location

Power supply units

A DD9500/DD9800 system has four power supply units, numbered PSU0, PSU1, PSU2, and PSU3 from left to right. Each power supply has its own integral cooling fan.

NOTE: The DD9500/DD9800 system should be powered from redundant AC sources. This allows one AC source to fail or be serviced without impacting system operation. PSU0 and PSU1 should be attached to one AC source. PSU2 and PSU3 should be attached to the other AC source.

The AC power plugs are located to the right of each power supply. The wire clips for the AC cords hold the cords in place. The wire clips must be disengaged before disconnecting the AC power to each power supply.

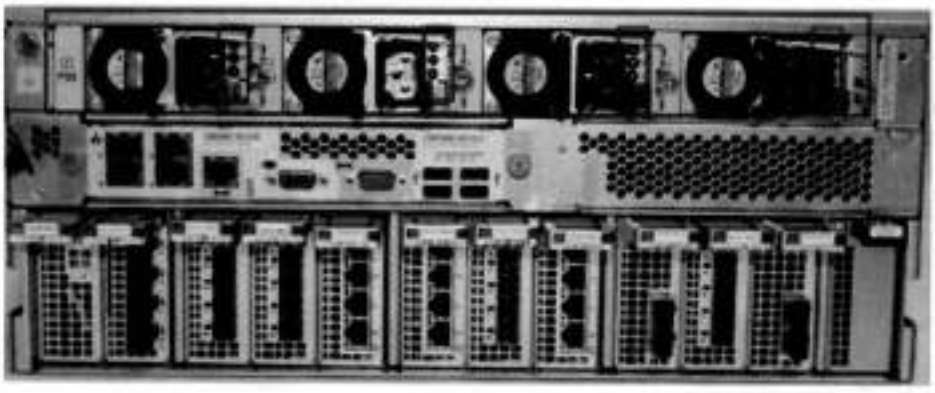


Figure 137. Four power supplies

Management module

The following figure shows the location of the management module on the rear of the system and identifies the interfaces.

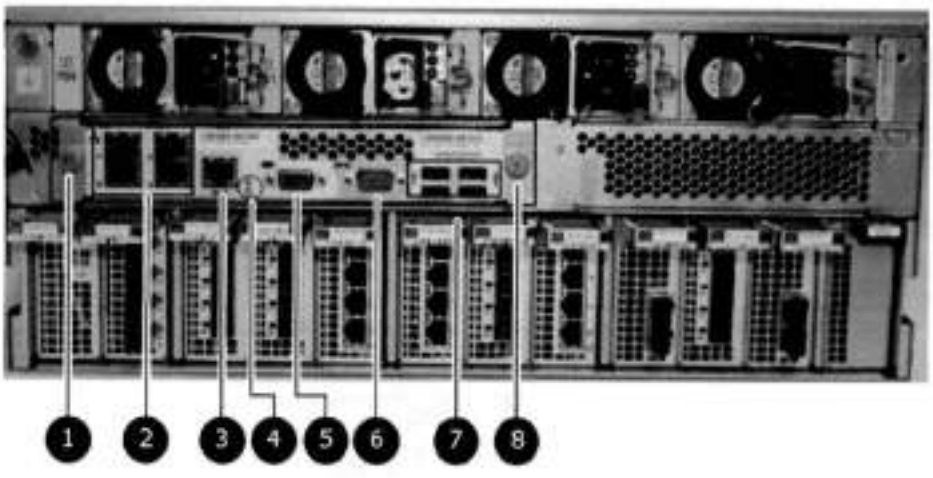


Figure 138. Management module

1. Left blue thumbscrew to loosen the management module
2. 4 x 1000BaseT Ethernet ports (For details, see the picture - 1000BaseT Ethernet ports)
3. Service network port (IPMI, 1000BaseT Ethernet port)
4. Service LED
5. VGA port
6. Serial port
7. Four USB ports
8. Right blue thumbscrew to loosen the management module

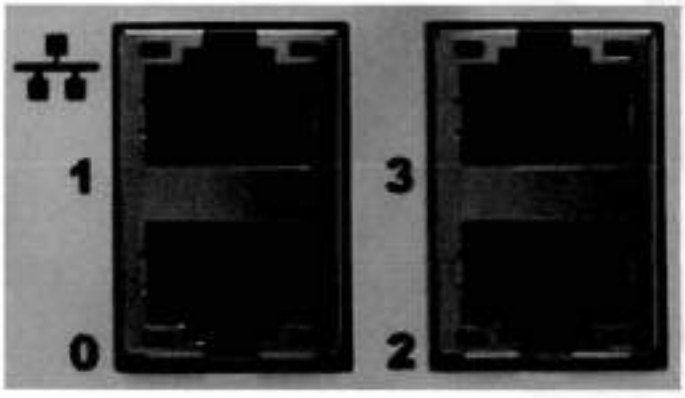


Figure 139. 1000BaseT Ethernet ports

- Lower left port: physical #0, logical ethMa
- Top left port: physical #1, logical ethMb
- Lower right port: physical #2, logical ethMc
- Top right port: physical #3, logical ethMd

Rear LED indicators

The rear elements containing LEDs include each power supply, each I/O module, and the management module.

The figure shows the rear LEDS.

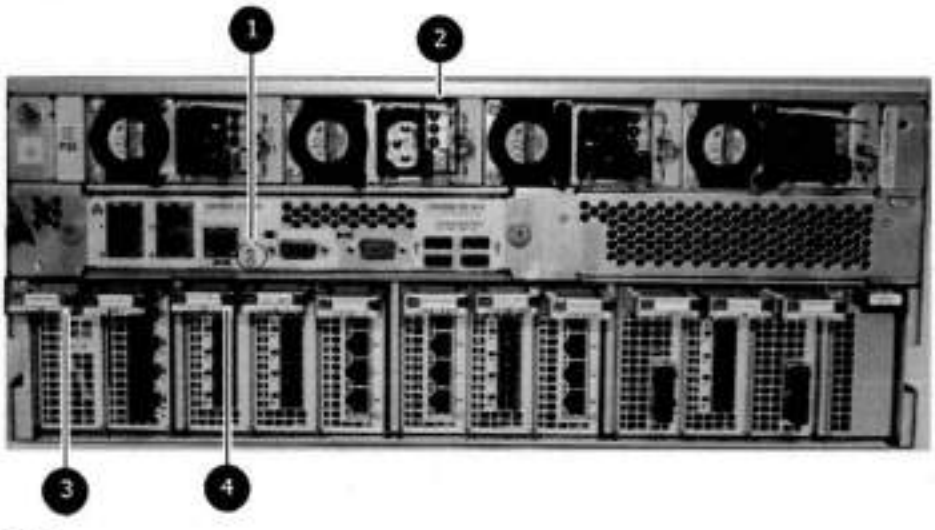


Figure 140. Rear LEDs

1. Management module service LEDs
2. Power supply LEDs
3. NVRAM LEDs
4. I/O Module LEDs

The power supply LEDs include:

- AC LED on top
- DC LED in the middle
- Service Required LED on the bottom

Figure 141. Power supply LEDs

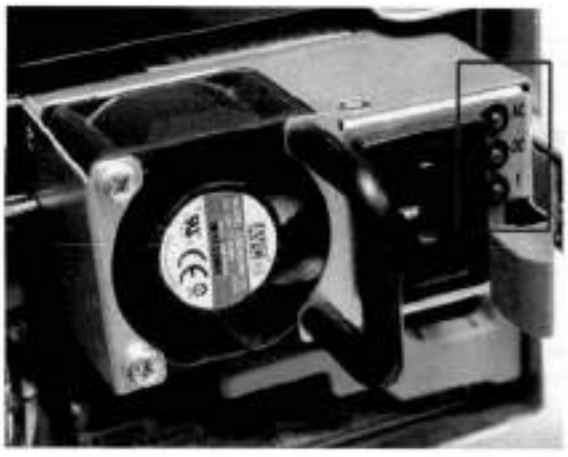


Table 163. Rear LED status indicators

Part	Description or Location	State
Power supply	AC LED	Steady green indicates normal AC input power.
Power supply	DC LED	Steady green indicates normal DC output power.
Power supply	Service LED	Solid amber indicates a failed power supply.
I/O module	I/O module handle	Solid green means I/O module functioning normally. Amber indicates a fault condition. Each I/O module also has per port LEDs. These LEDs are blue on the FC, and SAS I/O modules. They light when the port is active.
Management module	Bicolor LED	Solid green means management module functioning normally. Amber indicates that the management module requires service.

Available I/O modules

I/O modules may include:

- Quad port Ethernet 10GBase-SR Optical with LC connectors
- Quad port Ethernet 10GBase-CX1 Direct Attach Copper with SPF+ module
- Quad port Ethernet 10GBase-T Copper
- Dual port 16 Gbps Fibre Channel
- Quad port 6 Gbps SAS

I/O module port physical mapping

I/O module ports are numbered starting with 0. When the I/O modules are inserted vertically into the system chassis, port 0 is on the bottom.

I/O module port logical mapping

The numerical port labels on the I/O modules are identified logically in the DD OS software by the following descriptions:

- I/O module type
- I/O module slot

- Alphabetic character corresponding to the physical port number

The following example is based on a four-port Ethernet I/O module installed in slot 1 of the system chassis.

Table 164. Physical to logical port mapping example

Physical port	Logical identifier
0	eth1a
1	eth1b
2	eth1c
3	eth1d

Ethernet I/O module options

The available Ethernet I/O modules are:

- Dual Port 10GBase-SR Optical with LC connectors
- Dual Port 10GBase-CX1 Direct Attach Copper with SPF+ module
- Quad Port 1000Base-T Copper with RJ-45 connectors
- Quad port 2 port 1000Base-T Copper (RJ45) /2 port 1000Base-SR Optical

Fibre Channel I/O modules

A Fibre Channel (FC) I/O module is a dual-port Fibre Channel module. Up to four FC I/O modules may be installed. The optional virtual tape library (VTL) feature requires at least one FC I/O module. Boost over Fibre Channel is an optional feature and requires at least one FC I/O module. A maximum of four FC I/O modules may be installed in a system using either VTL or the Boost protocol or a combination of both protocols.

SAS I/O modules

DD9500 systems have three quad-port SAS I/O modules installed in slots 2, 3 and 6. Systems configured with DD Extended Retention (ER) or DD Cloud Tier software options require an additional SAS I/O module in slot 9.

I/O module slot assignments

The following figure shows the location of the NVRAM and I/O modules.

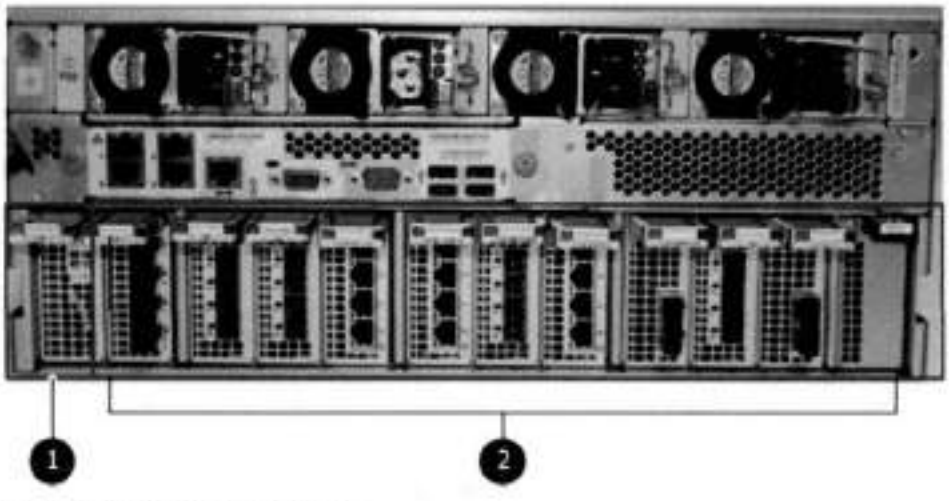


Figure 142. Location of NVRAM and I/O modules

1. NVRAM module—slot 0
2. I/O modules—slots 1 to 11 (See the I/O module slot assignments table.)

The table shows the I/O module slot assignments for the DD9500 system. Each type of I/O module is restricted to certain slots.

Table 165. DD9500 I/O module slot assignments

Slot	Base configuration	HA	ER or DD Cloud Tier	DD Cloud Tier and HA
0	NVRAM	NVRAM	NVRAM	NVRAM
1	Fibre Channel (FC), Ethernet or empty	Fibre Channel (FC), Ethernet or empty	Fibre Channel (FC), Ethernet or empty	Fibre Channel (FC), Ethernet or empty
2	SAS	SAS	SAS	SAS
3	SAS	SAS	SAS	SAS
4	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
5	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
6	SAS	SAS	SAS	SAS
7	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
8	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
9	Not available (contains a filler)	Not available (contains a filler)	SAS	SAS
10	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
11	FC, Ethernet or empty	10 Gb optical Ethernet for interconnect between the primary and standby nodes in the HA pair.	FC, Ethernet or empty	10 Gb optical Ethernet for interconnect between the primary and standby nodes in the HA pair.

Slot addition rules

This system has 12 slots for I/O modules. Slots 0, 2, 3, 6, 9, and 11 are reserved for mandatory I/O modules. Slots 1, 4, 5, 7, 8, and 10 support optional host interface I/O modules. The maximum supported number of any type of host interface (Ethernet or FC) I/O module is four.

NOTE: The maximum number of host interface I/O modules that are listed above does not include the 10 GbE Optical I/O module for the HA interconnect. The HA interconnect is a fifth Ethernet module, but it is reserved for communication between the two nodes of an HA pair, and is not available for host connections.

The maximum number of I/O modules, including both mandatory and optional I/O modules, supported in a system varies by configuration:

- Single node: 10
- HA: 10
- DD Extended Retention: 10
- DD Cloud Tier: 10
- HA + DD Cloud Tier: 11

Three I/O module slots are tied to each CPU in the system. When installing I/O modules, balance the load across the CPUs. The following table shows the CPU to slot mappings.

CPU	I/O module slots
0	0, 1, 2

CPU	I/O module slots
1	3, 4, 5
2	6, 7, 8
3	9, 10, 11

The following table assigns rules for populating the I/O modules.

Table 166. I/O module slot population rules

Step	I/O module type	Slots	Notes
1: Populate mandatory I/O modules	NVRAM	0	
	Quad Port SAS	2	
	Quad Port SAS	3	
	Quad Port SAS	6	
	Quad Port SAS	9	This slot remains empty if the system does not use DD Cloud Tier or DD Extended Retention.
	Quad Port 10GbE Optical	11	This slot remains empty if the system does not use HA.
2: Populate host interface I/O modules	• Quad Port 10GbE SR • Quad Port 10 GBase-T • Dual Port 16 Gbps Fibre Channel	1, 4, 5, 7, 8, 10	Install host interface I/O modules in the remaining slots. Install the I/O modules to balance the load across the CPUs. Do not place two Ethernet or two FC I/O modules on one CPU.[a]

a. HA systems are the exception to this guidance, as a Quad Port 10GbE SR I or Quad Port 10 GBase-T /O module can be added in slot 10 alongside the HA interconnect I/O module in slot 11.

Internal System Components

The storage processor (SP) is a subassembly within the chassis that contains the memory risers with the DIMMs and a fan tray with fan modules. The SP module also contains the 4 CPUs, which cannot be removed or replaced.

- The memory risers tray, which contains 8 memory risers with DIMMs, can be accessed from the front of the SP module. The memory risers are not hot swappable
- The fan tray, which contains 8 fan modules, can be accessed from the front of the SP module. The fans are hot swappable.

The DIMMS can be accessed by pulling the entire SP module away from the chassis. Depending on the model, there are DIMMs totaling:

- 256 GB or 512 GB for a DD9500 system.
- 256 GB or 768 GB for a DD9800 system.

The figures show the location of the SP module, the DIMM risers accessed from a partly removed SP module, and the fan tray partly removed.

Do not lift the DD9500/DD9800 system, or the storage processor (SP) module, or any modules by the handle. The handle is not designed to support the weight of the populated shelf. Also do not carry the DD9500/DD9800 system or the SP by the handle. The handles are only intended to be used to insert or remove the SP module.

Figure 143. SP module

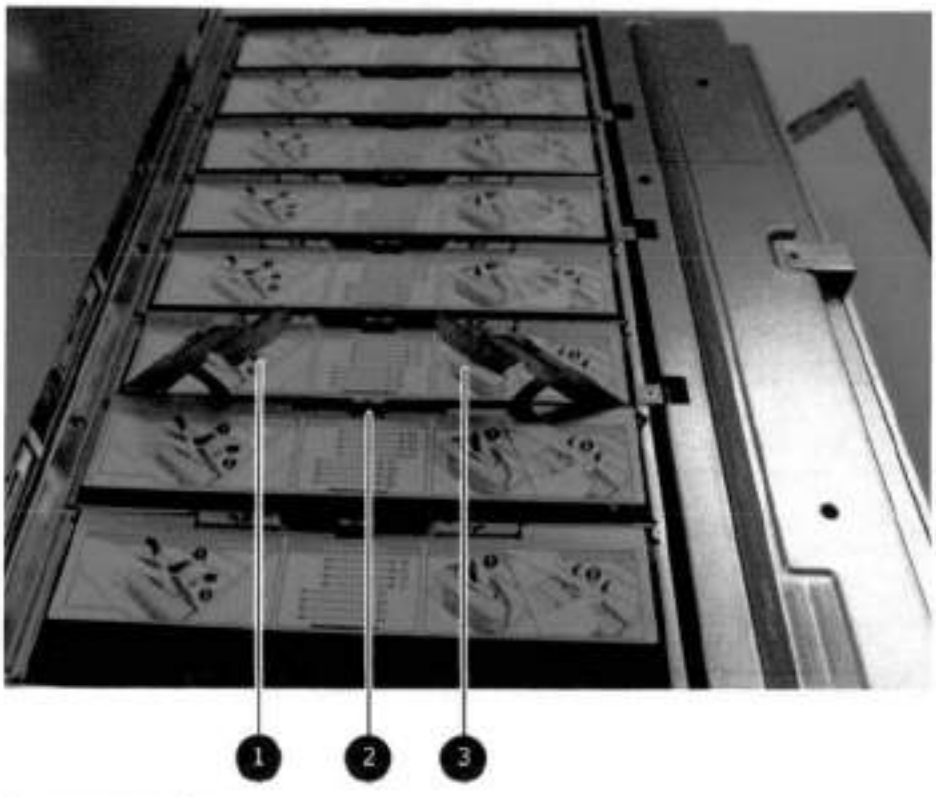


Figure 144. Releasing a memory riser

1. Left riser card ejector handle
2. Release button
3. Right riser card ejector handle

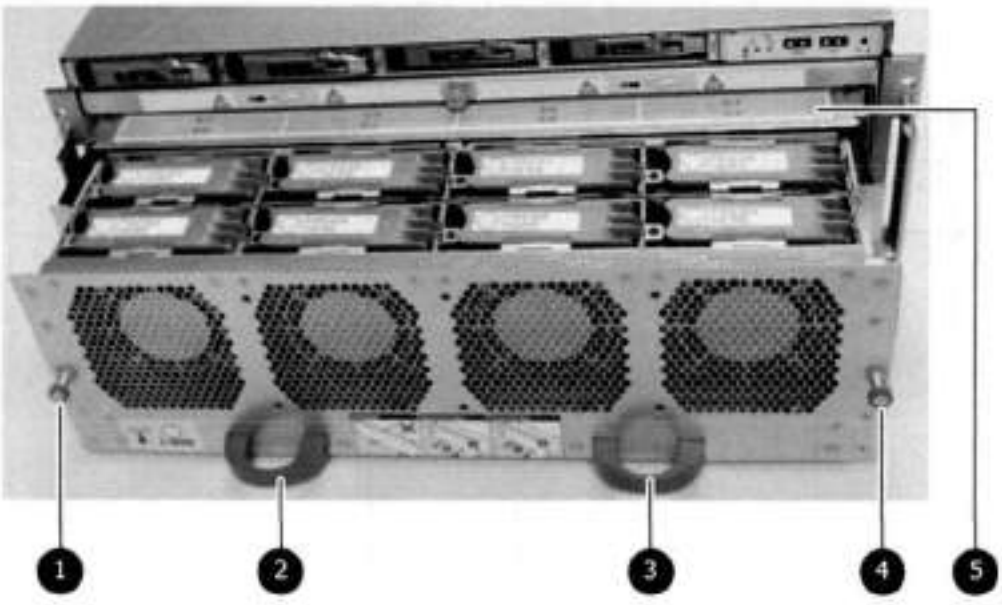


Figure 145. Open fan tray

NOTE: Do not loosen the blue thumbscrew on the SP latch handle to access the fan tray. Use the orange thumbscrews on the front as shown in the picture.

1. Left fan tray thumbscrew
2. Front panel left handle
3. Front panel right handle
4. Right fan tray thumbscrew
5. Location map of the fans

DIMM modules

The DD9500 system contains the following memory configurations:

Table 167. DD9500 memory configurations

System	Base	Expanded	ER/DD Cloud Tier
DD9500	32 x 8 GB DIMMs (256 GB)	32 x 8 GB DIMMs + 16 x 16 GB DIMMs (512 GB)	32 x 8 GB DIMMs + 16 x 16 GB DIMMs (512 GB)

Cooling fans

A system contains eight hot-swappable cooling fans in a 7+1 redundant configuration, which is located in the front of the system within a movable fan tray. The fans provide cooling for the processors, DIMMs, and I/O modules. Each fan has an LED which glows amber when the fan is failed or faulted. A system can run with one fan faulted.

DD9500 and ES30 shelf guidelines

The system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your system as listed in the following table below.
- Use the Installation and Setup Guide for your system to minimize the chance of a cabling mistake.
- A system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.

- DD9500 systems support ES30 SATA shelves after controller upgrades from older models.
- ES30 SATA shelves must be on their own chain.

Table 168. DD9500 and ES30 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	ES30 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB) [1]	Max RAW external capacity (TB) [2]
DD9500	256	3x4	SAS 30, 45, 60; SATA 15, 30, 45	5[3]	6	432	540
DD9500	512	3x4	SAS 30, 45, 60; SATA 15, 30, 45	5[3]	6	864	1080
DD9500 ER [4, 5]	512	4x4	SAS 30, 45, 60; SATA 15, 30, 45	7	8	1728	2160
DD9500 HA[6, 7]	256	3x4	SAS 30, 45, 60	5[3]	6	432	540
DD9500 HA[6, 7]	512	3x4	SAS 30, 45, 60	5[3]	6	864	1080
DD9500 w/ Cloud Tier	512	4x4	SAS 30, 45, 60; SATA 15, 30, 45	7	8	864 (max), additional 240 SAS dedicated to Cloud Tier	1080 (max), additional 300 SAS dedicated to Cloud Tier
DD9500 w/ HA and Cloud Tier	512	4x4	SAS 30, 45, 60	7	8	864 (max), additional 240 SAS dedicated to Cloud Tier	1080 (max), additional 300 SAS dedicated to Cloud Tier

1. This figure only counts drives that have user data in the shelves.

2. The raw capacity of an ES30 is 125% of the available capacity.

4. 5 shelves maximum with ES30, 4 is the recommended maximum. 4 shelves maximum with ES20, 3 is the recommended maximum.

5. The maximum shelf count for any specific drive/shelf size might be less than the product of max shelves x max shelves per set.

6. There is no support for ERSO on HA systems.

7. There is no support for HA with SATA drives.

Types of cabinets and power connections

The ES30 chassis is installed in two types of racks: 40U-C (existing racks) and the 40U-P (newer racks). The racks use one phase or 3-phase power connections.

3-Phase power connections for 40U-P (current racks)

Some environments use 3-phase power for 40U-P racks that are used for several systems. In those situations, it is desirable to balance the current draw across all three phases. The recommended 3-phase power cabling attempts to do that, but an optimal configuration depends on the specific installation.

Cabling shelves

NOTE:

- Before cabling the shelves, physically install all shelves in the racks. Refer to the rail kit installation instructions included with the ES30 shelf for rack mounting.
- The documentation refers to two SAS HBAs. If only one HBA is allowed in a system, then use another port as defined later for that specific system.
- On an HA system, add cables from the second node to open ports at the end of the sets. The ports on the second node must connect to the same sets as the corresponding ports on the first node.

Ports on the system's SAS HBA cards connect directly to a shelf controller's host port. For redundancy, you need to create dual paths by using a port on one SAS HBA card to connect to one shelf controller in each shelf set, and a port on another SAS HBA card to connect to another shelf controller in the same shelf set. With dual paths, if one SAS HBA card fails, the shelf is still operational. However, in the unlikely event any single shelf becomes completely disconnected from power or SAS cables and becomes disconnected from a previously operational shelf, the file system goes down and the shelf is not operational. This is considered a double failure.

There are two kinds of configurations: one shelf in a set or multiple shelves in a set.

DD9500 and cabling

NOTE: If a system installation does not follow ALL of these rules, it is not a legitimate configuration.

Prerequisites:

- Follow the minimum and maximum shelf capacity configuration provided in the table.
- You cannot have ES30 SATA and ES30 SAS shelves in the same set.
- You cannot exceed the maximum amount of raw capacity displayed in the product's cabling table.
- You cannot exceed the maximum number of shelves displayed in the product's cabling table.
- You cannot have more than five ES30s in a single set (maximum of four is preferred).
- You can have seven ES30s for systems with Extended Retention software.
- There are no specific placement or cabling requirements for SSD shelves, or the metadata shelves for Cloud Tier configurations. These shelves can be installed and cabled the same way as standard ES30 shelves.

Table 169. Minimum and maximum configurations

System	DD9500	DD9500 w/	
Appliance	864 TB usable	864 TB usable	1008 TB usable
Minimum appliance shelf count	4	4	4
Maximum appliance shelf count	30	30	30
Extended Retention systems (ER)	1728 TB usable	2016 TB usable	2016 TB usable
Maximum shelves for ER	56	56	56
High Availability systems (HA)	864 TB usable	1008 TB usable	1008 TB usable
Maximum shelves for HA	42	42	47
Cloud Tier systems	1104 TB usable	1248 TB usable	1248 TB usable
Maximum shelves for Cloud Tier	42	42	47

The DD9500 base (non-Extended Retention) and HA systems supports six chains.

The following figures show cabling for base systems, HA systems, and systems with the Extended Retention software option.

NOTE: The racks are filled from bottom up.

DD9500 and DS60 shelf guidelines

The system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your system as listed in the following table.
- For redundancy, the two connections from a system to a set of shelves must use ports on different SAS I/O modules.
- Use the Installation and Setup Guide for your system to minimize the chance of a cabling mistake.
- A system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.
- ES30 SATA shelves must be on their own chain.
- If ES30 SAS shelves are on the same chain as a DS60, the maximum number of shelves on that chain is 5.

Table 170. DD9500 and DS60 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	DS60 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB)[1]	Max RAW external capacity (TB)
DD9500	256	3x4	SAS 45, 60	4	6	432	540
DD9500 Expanded	512	3x4	SAS 45, 60	4	6	864	1080
DD9500 ER	512	4x4	SAS 45, 60	4	8	1728	2160
DD9500 HA [2]	512	3x4	SAS 45, 60	4	6	864	1080
DD9500 Cloud Tier [3,4]	512	4x4	SAS 45, 60	4	8	864 + 240 for Cloud Tier	1080 + 300 for Cloud Tier
DD9500 Cloud Tier w/ HA [3,4]	512	4x4	SAS 45, 60	4	8	864 + 240 for Cloud Tier	1080 + 300 for Cloud Tier

NOTE: An entry of 45 corresponds to DS60-3 models and an entry of 60 corresponds to DS60-4 models.

1. This column only counts drives that have user data in the shelves. For example, a DS60 4-240 has 192TB.

2. DD9300 base support 2.5 DS60-4 180 x 2 plus DS60 2 60, if a half- filled DS60 is necessary.

3. DD9300 Expanded supports five DS60 maximum.

4. There is no support for HA with SATA drives.

3-phase power connections for 40U-P (current racks)

Some environments use 3-phase power for 40U-P racks used for several systems. In those situations it is desirable to balance the current draw across all 3 phases. The recommended 3-phase power cabling attempts to do that, but an optimal configuration is dependent on the specific installation.

DD9500 and DD9800 cabling

NOTE: If a system installation does not follow ALL of these rules, it is not a legitimate configuration.

Prerequisites:

- Follow the minimum and maximum shelf capacity configuration provided in the table.
- You cannot have ES30 SATA and ES30 SAS shelves in the same set.
- You cannot exceed the maximum amount of raw capacity displayed in the product's cabling table.
- You cannot exceed the maximum number of shelves displayed in the product's cabling table.

- You cannot have more than five ES30s in a single set (maximum of four is preferred).
- You can have seven ES30s for systems with Extended Retention software.
- There are no specific placement or cabling requirements for SSD shelves, or the metadata shelves for Cloud Tier configurations. These shelves can be installed and cabled the same way as standard ES30 shelves.

Table 171. Minimum and maximum configurations

System	DD9500	DD9500 w/	
Appliance	864 TB usable	864 TB usable	1008 TB usable
Minimum appliance shelf count	4	4	4
Maximum appliance shelf count	30	30	30
Extended Retention systems (ER)	1728 TB usable	2016 TB usable	2016 TB usable
Maximum shelves for ER	56	56	56
High Availability systems (HA)	864 TB usable	1008 TB usable	1008 TB usable
Maximum shelves for HA	42	42	47
Cloud Tier systems	1104 TB usable	1248 TB usable	1248 TB usable
Maximum shelves for Cloud Tier	42	42	47

The DD9500 base (non-Extended Retention) and HA systems supports six chains.

The following figures show cabling for base systems, HA systems, and systems with the Extended Retention software option.

NOTE: The racks are filled from bottom up.

13

DD9800

This chapter contains the following topics:

Topics:

- DD9800 system features
- DD9800 system specifications
- DD9800 storage capacity
- DD9800 front panel
- Rear panel
- I/O module slot assignments
- Internal system components
- DD9800 and ES30 shelf guidelines
- DD9800 and DS60 shelf guidelines

DD9800 system features

Table 172. DD9800 system features

Feature		DD9800 (Base configuration)	DD9800 (Expanded configuration)
Rack height		4U, supported in four-post racks only	4U, supported in four-post racks only
Rack mounting		Rack mount kit included with each system. Adjustable between 24 - 36 in. (60.9–76.2 cm).	Rack mount kit included with each system. Adjustable between 24 - 36 in. (60.9–76.2 cm).
Power		4 hot-swappable power units, 2 pairs of 1 +1 redundant	4 hot-swappable power units, 2 pairs of 1 +1 redundant
Voltage		200–240 V~. Frequency: 50 Hz to 60 Hz.	200–240 V~. Frequency: 50 Hz to 60 Hz.
Processor		4 Intel EX processors.	4 Intel EX processors.
NVRAM		One 8-GB NVRAM module for data integrity during a power outage	One 8-GB NVRAM module for data integrity during a power outage
Fans		8 hot-swappable fans, redundant	8 hot-swappable fans, redundant
Memory		32 x 8 GB DIMM (256 GB)	32 x 8 GB DIMM + 32 x 16 GB DIMM (768 GB)
Internal drives		4 x 400 GB (base 10) hot-swappable solid state drives (SSD)	4 x 400 GB (base 10) hot-swappable solid state drives (SSD)
I/O module slots		11 I/O module (Fibre Channel, Ethernet, and SAS) slots. Replaceable I/O modules are not hot-swappable. See I/O module slot assignments	11 I/O module (Fibre Channel, Ethernet, and SAS) slots. Replaceable I/O modules are not hot-swappable. See I/O module slot assignments
Supported capacity	Non-extended retention	630 TB	1260 TB
	DD Cloud Tier	N/A	2520 TB [a]
	Extended retention	N/A	1260 TB [b]
High availability support		Yes	Yes
HA private interconnect		4 10 GbE optical ports	4 10 GbE optical ports
External SSD shelf		1 x 8 drive SSD shelf	1 x 15 drive SSD shelf

a. DD Cloud Tier requires five ES30 shelves fully populated with 4 TB drives to store DD Cloud Tier metadata.
b. Extended retention not available on HA configurations

DD9800 system specifications

Table 173. DD9800 system specifications

Model	Watts	BTU/hr	Power (VA)	Weight	Width	Depth	Height
DD9800	1887	6444	1981	117 lb / 53.2 kg	19 in / 48.3 cm	29.5 in / 74.9 cm	7 in / 17.8 cm

- Operating temperature: 50° to 95° F (10° to 35° C), derate 1.1° C per 1000 feet, above 7500 feet up to 10,000 feet
- Operating humidity: 20% to 80%, non-condensing
- Non-operating temperature: -40° to +149° F (-40° to +65° C)
- Operating acoustic noise: Sound power, LWAd, is 7.7 bels.

DD9800 storage capacity

The table lists the capacities of the systems. The internal indexes and other product components use variable amounts of storage, depending on the type of data and the sizes of files. If you send different datasets to otherwise identical systems, one system may, over time, have room for more or less actual backup data than another.

NOTE: System commands compute and display amounts of disk space or data as decimal multiples of certain powers of two (2^{10}, 2^{20}, 2^{30}, and so forth). For example, 7 GB of disk space = 7 x 2^{30} bytes = 7 x 1,073,741,824 bytes. The system sees this process as Base 2 calculation.

Table 174. DD9800 storage capacity

System/ Installed Memory	Internal Disks	Raw Storage (Base 10)	Data Storage Space (Base 2 Calculation)	Data Storage Space (Base 10 Calculation)
DD9800 (3 SAS I/O modules) 256 GB	2.5 in.: 4 x 400 GB SATA SSD No User Data	630 TB (external)	457.8 TiB	504 TB
DD9800 (3 SAS I/O modules) 768 GB	2.5 in.: 4 x 400 GB SATA SSD No User Data	1,260 TB (external)	915.6 TiB	1,008 TB
DD9800 with DD Cloud Tier (4 SAS I/O modules) 768 GB	2.5 in.: 4 x 400 GB SATA SSD No User Data	3,780 TB (external)	2746.8 TiB	3,024 TB
DD9800 with ER (4 SAS I/O modules) 768 GB	2.5 in.: 4 x 400 GB SATA SSD No User Data	2,520 TB (external)	1,831.2 TiB	2,016 TB

Table 175. DD9800 with ES30 SAS shelves

	DD9800	DD9800
Memory (GB)	256	768
SAS I/O modules x ports per module	3x4	3x4
ES30 support (TB)	SAS 30, 45, 60	SAS 30, 45, 60
Maximum shelves per set	5	5
Maximum number of sets	6	6

NOTE: ES30 SATA shelves are supported when upgrading from an older single node system, but are not supported with HA pairs or new installations.

Table 176. DD9800 with DS60 shelves

	DD9800	DD9800
Memory (GB)	256	768
SAS I/O modules x ports per module	3x4	3x4
DS60 support (TB)	SAS 45, 60	SAS 45, 60
Maximum shelves per set	4	4
Maximum number of sets	6	6

DD9800 front panel

The four solid state drives (SSDs), the storage processor (SP), and the fans are accessed from the front of the system. The SP must be pulled out to provide access to the DIMMs. The fans are accessed without pulling or removing the SP and they are hot-swappable. The photo shows the interfaces on the front of the system.

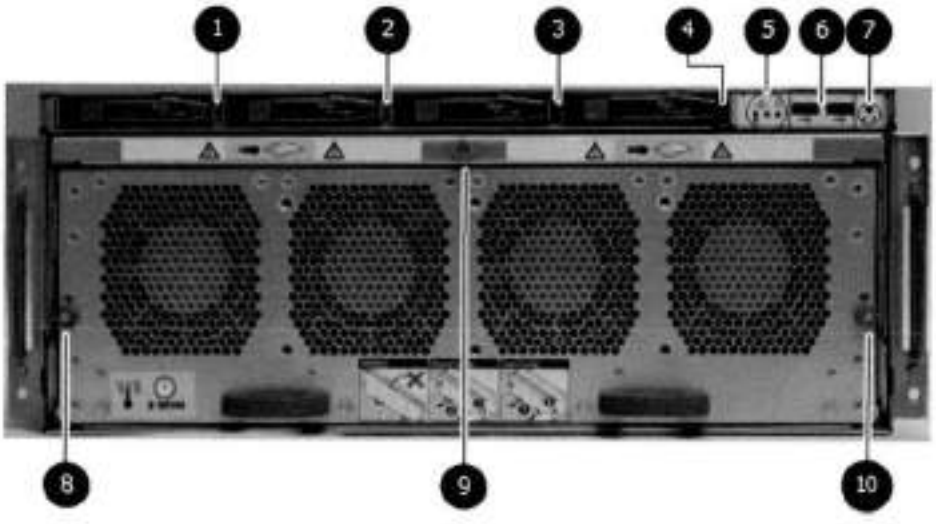


Figure 146. Front panel components

1. SSD slot 0
2. SSD slot 1
3. SSD slot 2
4. SSD slot 3
5. Front LEDs
6. USB ports
7. Power button
8. Fan tray thumbscrew (left)
9. SP module thumbscrew to secure the ejector handle
10. Fan tray thumbscrew (right)

Front LED indicators

On the front panel to the right of SSD #4 (in Slot 3) are 3 LEDs that show high level system status. The System Power LED glows blue to show the system is powered on.

NOTE: The system can have power (be plugged in) but the blue LEDs are off if the system is powered off.

The SP Service LED is normally off, but glows amber wherever the storage processor (SP) requires service. The Enclosure Service LED is normally off, but glows amber whenever the SP or other replaceable parts require service. The System Power and Enclosure Service LEDs are visible through the front bezel.

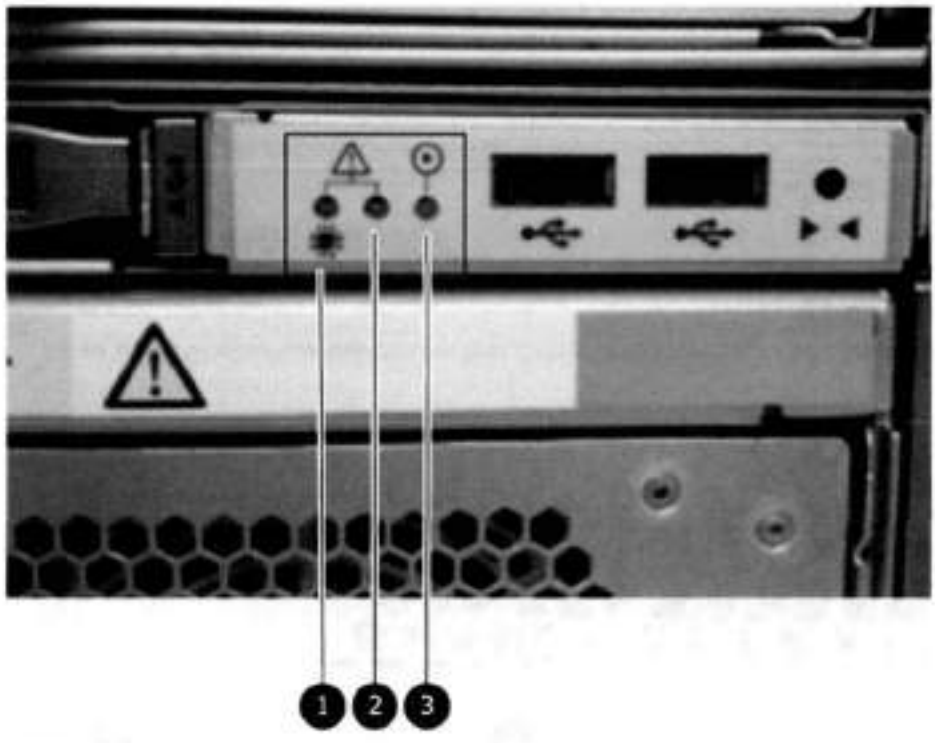


Figure 147. Service LEDs

1. SP service LED — Amber light indicates that the SP or one of its components needs service.
2. Enclosure Service LED — This is normally off, but amber light indicates that the enclosure or something within the enclosure— the fans, SP, I/O modules, management module etc—requires service.
3. System power LED — Blue light indicates system running

The power button shown in the picture is used when a system needs to be powered up after a shut down using the `system poweroff` command. Once power is restored the system power LED light turns blue.

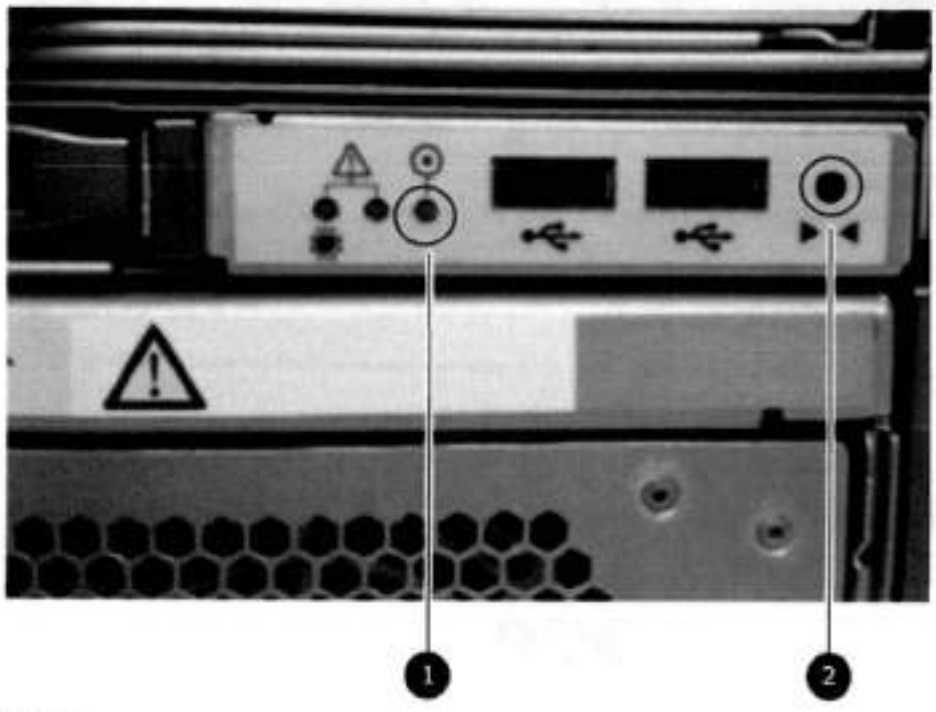


Figure 148. Power button

1. System power LED — Blue light indicates system running
2. Power button

The LEDs in the front are shown in the following figure.

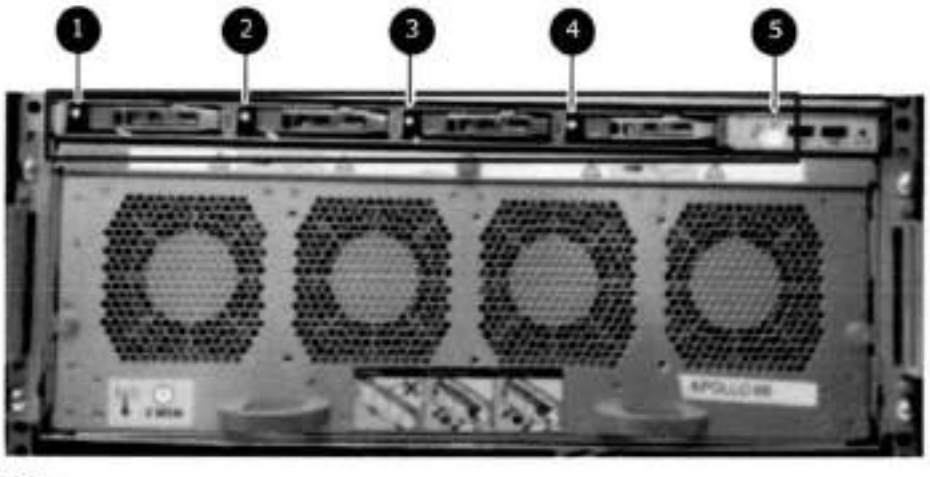


Figure 149. Front LEDs

1. SSD LED in slot 0
2. SSD LED in slot 1
3. SSD LED in slot 2
4. SSD LED in slot 3
5. System power LED — Blue light indicates system running

Table 177. Front panel LED status indicators

Part	Description or Location	State
System, SP fault	Exclamation point within a triangle	Dark indicates normal operation. Amber indicates failure.
System, chassis fault	Exclamation point within a triangle	Dark indicates normal operation. Amber indicates a fault condition.
SSD	Top LED	Solid blue, disk ready, blinks while busy.
SSD	Bottom LED	Dark indicates healthy. Solid amber indicates disk fail.

Solid-state drives

A system contains 4 hot-swappable 2.5 in. 400 GB solid-state drives (SSD) located in the front. There are four drive bays numbered 0–3 from left to right. A dual drive failure allows the system to operate without disruption.

Each drive has a blue colored power LED and an amber fault LED.

Figure 150. SSD drives

1. Slot 0
2. Slot 1
3. Slot 2
4. Slot 3

Rear panel

In the rear of the system, the top section contains the 4 power supply units. In the middle of the section, on the left, is serial number tag location. To the right of the serial number tag location is the management module. The lower section contains the NVRAM and the I/O modules numbered 0 through 11 from left to right. The photo shows the hardware features and interfaces on the rear of the system.

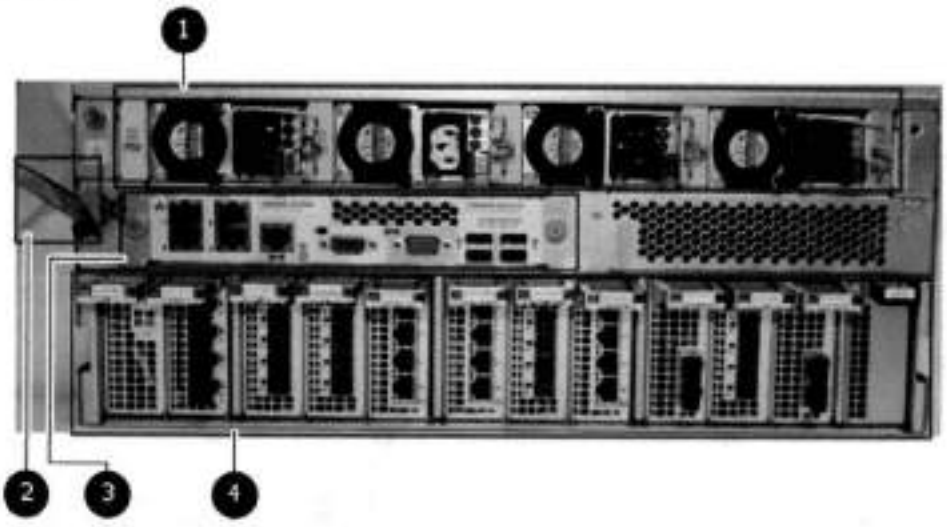


Figure 151. Features on rear of chassis

1. Power supply units
2. Serial number tag
3. Management module
4. NVRAM and I/O modules (slots 0-11)

The figure shows the location of the serial number tag on the left of the management module.

Figure 152. Serial number tag location

Power supply units

A DD9800 system has four power supply units, numbered PSU0, PSU1, PSU2, and PSU3 from left to right. Each power supply has its own integral cooling fan.

NOTE: The DD9800 system should be powered from redundant AC sources. This allows one AC source to fail or be serviced without impacting system operation. PSU0 and PSU1 should be attached to one AC source. PSU2 and PSU3 should be attached to the other AC source.

The AC power plugs are located to the right of each power supply. The wire clips for the AC cords hold the cords in place. The wire clips must be disengaged before disconnecting the AC power to each power supply.

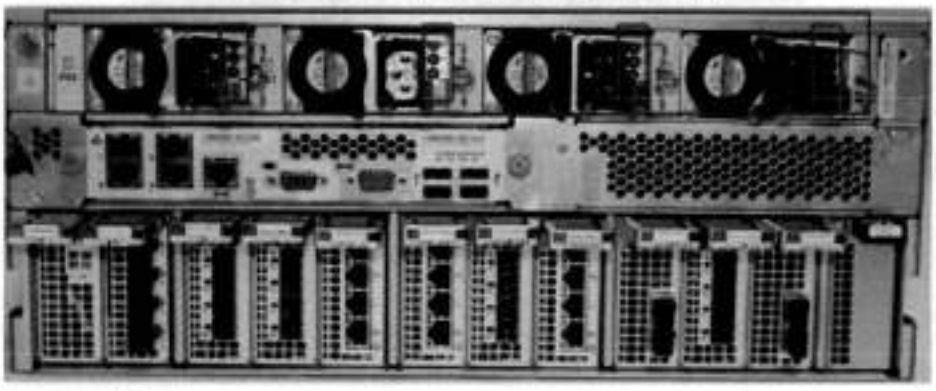


Figure 153. Four power supplies

Management module

The following figure shows the location of the management module on the rear of the system and identifies the interfaces.

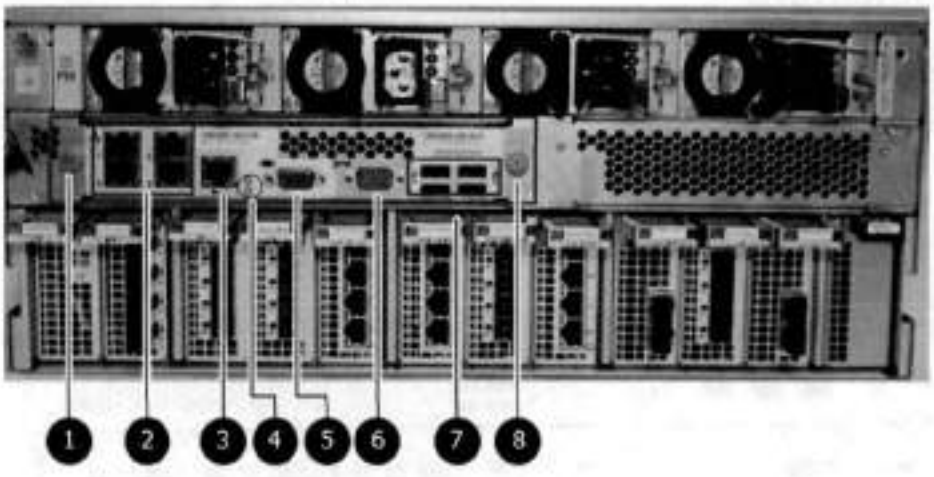


Figure 154. Management module

1. Left blue thumbscrew to loosen the management module
2. 4 x 1000BaseT Ethernet ports (For details, see the picture - 1000BaseT Ethernet ports)
3. Service network port (IPMI, 1000BaseT Ethernet port)
4. Service LED
5. VGA port
6. Serial port
7. Four USB ports
8. Right blue thumbscrew to loosen the management module

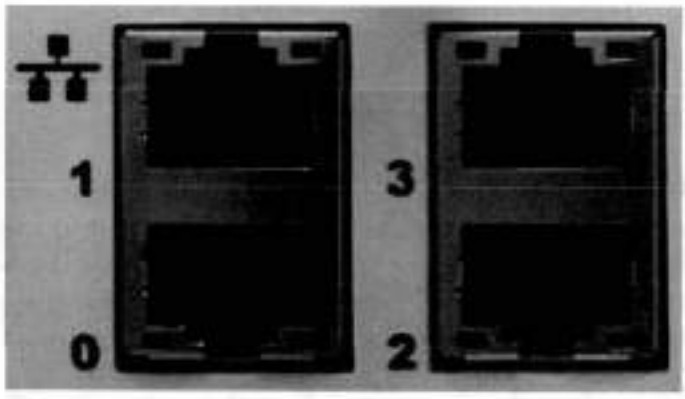


Figure 155. 1000BaseT Ethernet ports

- Lower left port: physical #0, logical ethMa
- Top left port: physical #1, logical ethMb
- Lower right port: physical #2, logical ethMc
- Top right port: physical #3, logical ethMd

Rear LED indicators

The rear elements containing LEDs include each power supply, each I/O module, and the management module.

The figure shows the rear LEDS.

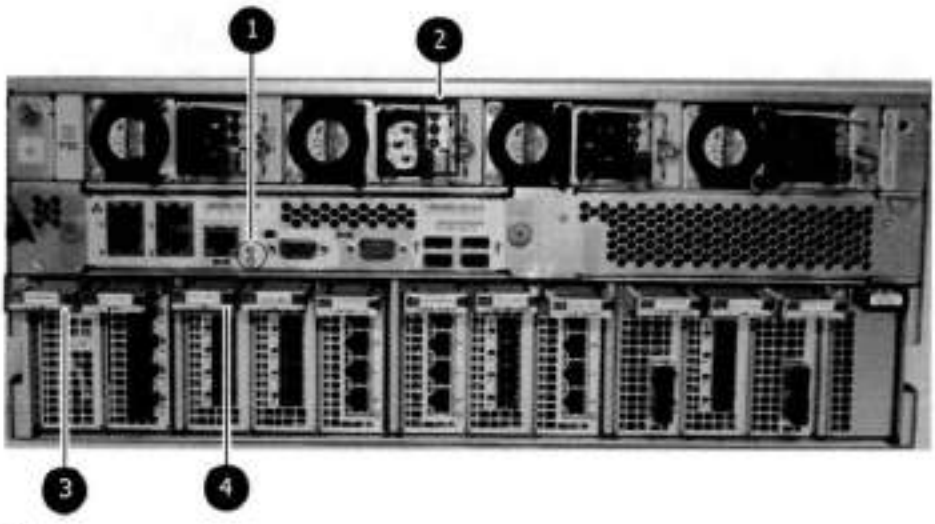


Figure 156. Rear LEDs

1. Management module service LEDs
2. Power supply LEDs
3. NVRAM LEDs
4. I/O Module LEDs

The power supply LEDs include:

- AC LED on top
- DC LED in the middle
- Service Required LED on the bottom

Figure 157. Power supply LEDs

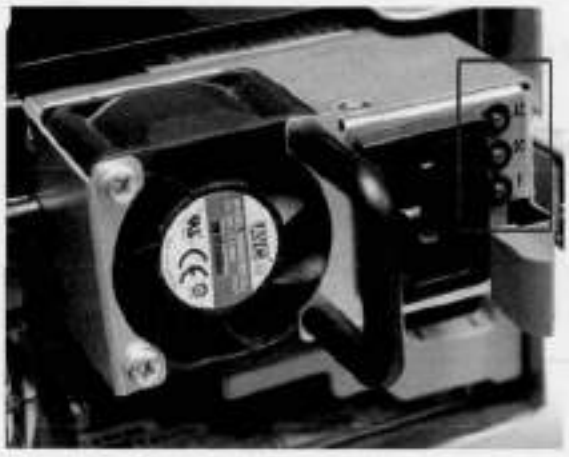


Table 178. Rear LED status indicators

Part	Description or Location	State
Power supply	AC LED	Steady green indicates normal AC input power.
Power supply	DC LED	Steady green indicates normal DC output power.
Power supply	Service LED	Solid amber indicates a failed power supply.
I/O module	I/O module handle	Solid green means I/O module functioning normally. Amber indicates a fault condition. Each I/O module also has per port LEDs. These LEDs are blue on the FC, and SAS I/O modules. They light when the port is active.
Management module	Bicolor LED	Solid green means management module functioning normally. Amber indicates that the management module requires service.

Available I/O modules

I/O modules may include:

- Quad port Ethernet 10GBase-SR Optical with LC connectors
- Quad port Ethernet 10GBase-CX1 Direct Attach Copper with SFF+ module
- Quad port Ethernet 10GBase-T Copper
- Dual port 16 Gbps Fibre Channel
- Quad port 6 Gbps SAS

I/O module port physical mapping

I/O module ports are numbered starting with 0. When the I/O modules are inserted vertically into the system chassis, port 0 is on the bottom.

I/O module port logical mapping

The numerical port labels on the I/O modules are identified logically in the DD OS software by the following descriptions:

- I/O module type
- I/O module slot

- Alphabetic character corresponding to the physical port number

The following example is based on a four-port Ethernet I/O module installed in slot 1 of the system chassis.

Table 179. Physical to logical port mapping example

Physical port	Logical identifier
0	eth1a
1	eth1b
2	eth1c
3	eth1d

Ethernet I/O module options

The available Ethernet I/O modules are:

- Dual Port 10GBase-SR Optical with LC connectors
- Dual Port 10GBase-CX1 Direct Attach Copper with SPF+ module
- Quad Port 1000Base-T Copper with RJ-45 connectors
- Quad port 2 port 1000Base-T Copper (RJ45) /2 port 1000Bese-SR Optical

Fibre Channel I/O modules

A Fibre Channel (FC) I/O module is a dual-port Fibre Channel module. Up to four FC I/O modules may be installed. The optional virtual tape library (VTL) feature requires at least one FC I/O module. Boost over Fibre Channel is an optional feature and requires at least one FC I/O module. A maximum of four FC I/O modules may be installed in a system using either VTL or the Boost protocol or a combination of both protocols.

SAS I/O modules

DD9800 systems have three quad-port SAS I/O modules installed in slots 2, 3 and 6. Systems configured with DD Extended Retention (ER) or DD Cloud Tier software options require an additional SAS I/O module in slot 9.

I/O module slot assignments

The following figure shows the location of the NVRAM and I/O modules.

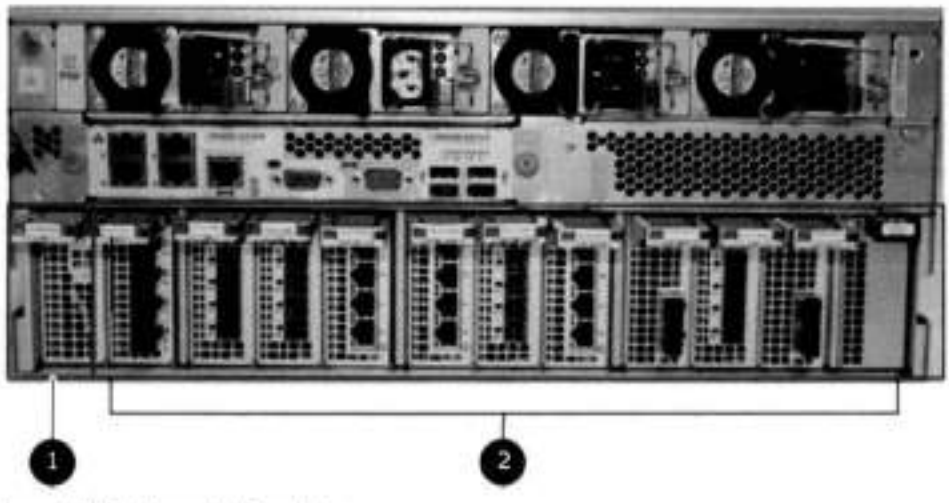


Figure 158. Location of NVRAM and I/O modules

1. NVRAM module—slot 0
2. I/O modules—slots 1 to 11 (See the I/O module slot assignments table.)

The table shows the I/O module slot assignments for the DD9800 system. Each type of I/O module is restricted to certain slots.

Table 180. DD9800 I/O module slot assignments

Slot	Base configuration	HA	ER or DD Cloud Tier	DD Cloud Tier and HA
0	NVRAM	NVRAM	NVRAM	NVRAM
1	Fibre Channel (FC), Ethernet or empty	Fibre Channel (FC), Ethernet or empty	Fibre Channel (FC), Ethernet or empty	Fibre Channel (FC), Ethernet or empty
2	SAS	SAS	SAS	SAS
3	SAS	SAS	SAS	SAS
4	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
5	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
6	SAS	SAS	SAS	SAS
7	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
8	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
9	Not available (contains a filler)	Not available (contains a filler)	SAS	SAS
10	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty	FC, Ethernet or empty
11	FC, Ethernet or empty	10 Gb optical Ethernet for interconnect between the primary and standby nodes in the HA pair.	FC, Ethernet or empty	10 Gb optical Ethernet for interconnect between the primary and standby nodes in the HA pair.

Slot addition rules

This system has 12 slots for I/O modules. Slots 0, 2, 3, 6, 9, and 11 are reserved for mandatory I/O modules. Slots 1, 4, 5, 7, 8, and 10 support optional host interface I/O modules. The maximum supported number of any type of host interface (Ethernet or FC) I/O module is four.

NOTE: The maximum number of host interface I/O modules that are listed above does not include the 10 GbE Optical I/O module for the HA interconnect. The HA interconnect is a fifth Ethernet module, but it is reserved for communication between the two nodes of an HA pair, and is not available for host connections.

The maximum number of I/O modules, including both mandatory and optional I/O modules, supported in a system varies by configuration:

- Single node: 10
- HA: 10
- DD Extended Retention: 10
- DD Cloud Tier: 10
- HA + DD Cloud Tier: 11

Three I/O module slots are tied to each CPU in the system. When installing I/O modules, balance the load across the CPUs. The following table shows the CPU to slot mappings.

CPU	I/O module slots
0	0, 1, 2

CPU	I/O module slots
1	3, 4, 5
2	6, 7, 8
3	9, 10, 11

The following table assigns rules for populating the I/O modules.

Table 181. I/O module slot population rules

Step	I/O module type	Slots	Notes
1: Populate mandatory I/O modules	NVRAM	0	
	Quad Port SAS	2	
	Quad Port SAS	3	
	Quad Port SAS	6	
	Quad Port SAS	9	This slot remains empty if the system does not use DD Cloud Tier or DD Extended Retention.
	Quad Port 10GbE Optical	11	This slot remains empty if the system does not use HA.
2: Populate host interface I/O modules	• Quad Port 10GbE SR • Quad Port 10 GBase-T • Dual Port 16 Gbps Fibre Channel	1, 4, 5, 7, 8, 10	Install host interface I/O modules in the remaining slots. Install the I/O modules to balance the load across the CPUs. Do not place two Ethernet or two FC I/O modules on one CPU.[a]

a. HA systems are the exception to this guidance, as a Quad Port 10GbE SR I or Quad Port 10 GBase-T /O module can be added in slot 10 alongside the HA interconnect I/O module in slot 11.

Internal system components

The storage processor (SP) is a subassembly within the chassis that contains the memory risers with the DIMMs and a fan tray with fan modules. The SP module also contains the 4 CPUs, which cannot be removed or replaced.

- The memory risers tray, which contains 8 memory risers with DIMMs, can be accessed from the front of the SP module. The memory risers are not hot swappable
- The fan tray, which contains 8 fan modules, can be accessed from the front of the SP module. The fans are hot swappable.

The DIMMS can be accessed by pulling the entire SP module away from the chassis. Depending on the model, there are DIMMs totaling 256 GB or 768 GB.

The figures show the location of the SP module, the DIMM risers accessed from a partly removed SP module, and the fan tray partly removed.

Do not lift the DD9800 system, or the storage processor (SP) module, or any modules by the handle. The handle is not designed to support the weight of the populated shelf. Also do not carry the DD9800 system or the SP by the handle. The handles are only intended to be used to insert or remove the SP module.

Figure 159. SP module

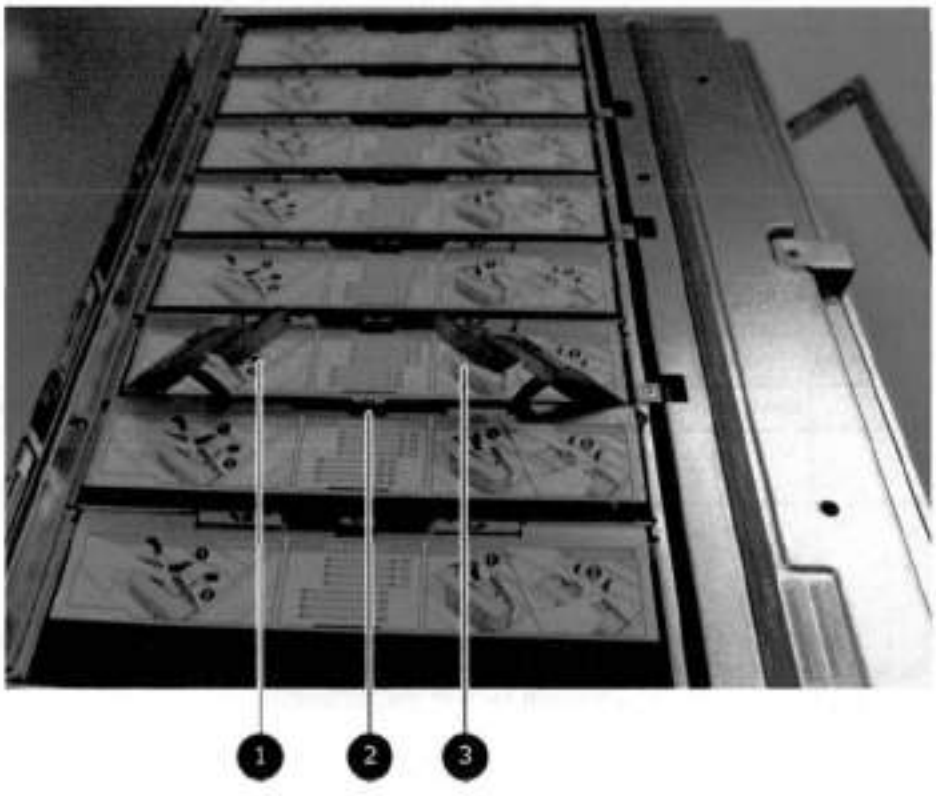


Figure 160. Releasing a memory riser

1. Left riser card ejector handle
2. Release button
3. Right riser card ejector handle

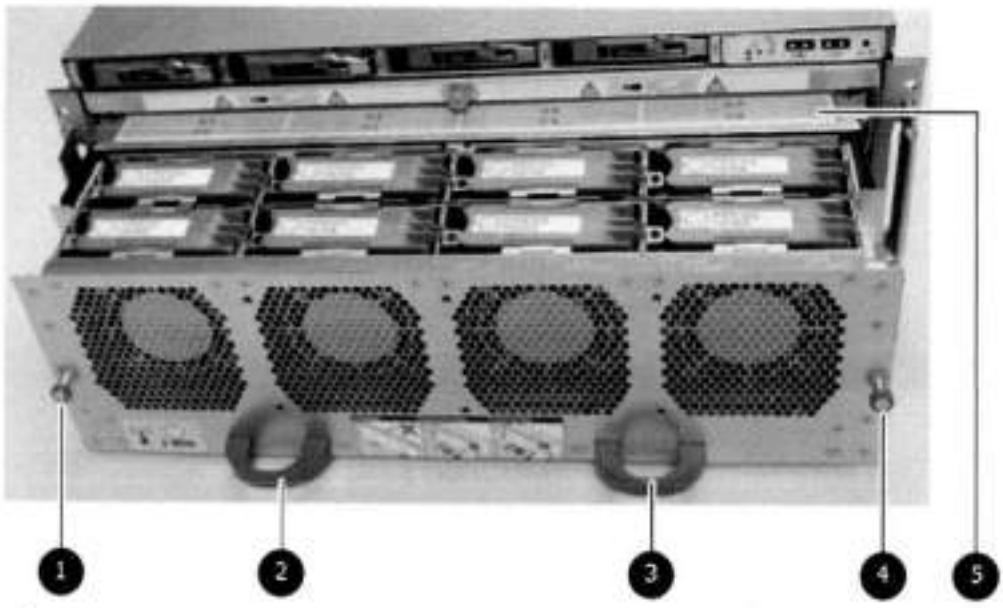


Figure 161. Open fan tray

NOTE: Do not loosen the blue thumbscrew on the SP latch handle to access the fan tray. Use the orange thumbscrews on the front as shown in the picture.

1. Left fan tray thumbscrew
2. Front panel left handle
3. Front panel right handle
4. Right fan tray thumbscrew
5. Location map of the fans

DIMM modules

The DD9800 system contains the following memory configurations:

Table 182. DD9800 memory configurations

System	Base	Expanded	ER/DD Cloud Tier
DD9800	32 x 8 GB DIMMs (256 GB)	32 x 8 GB DIMMs + 32 x 16 GB DIMMS (768 GB)	32 x 8 GB DIMMs + 32 x 16 GB DIMMS (768 GB)

Cooling fans

A system contains eight hot-swappable cooling fans in a 7+1 redundant configuration, which is located in the front of the system within a movable fan tray. The fans provide cooling for the processors, DIMMs, and I/O modules. Each fan has an LED which glows amber when the fan is failed or faulted. A system can run with one fan faulted.

DD9800 and ES30 shelf guidelines

The system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your system as listed in the following table below.
- Use the Installation and Setup Guide for your system to minimize the chance of a cabling mistake.
- A system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.

- ES30 SATA shelves must be on their own chain.

Table 183. DD9800 and ES30 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	ES30 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB) [1]	Max RAW external capacity (TB) [2]
DD9800 [3]	256	3x4	SAS 30, 45, 60; SATA 15, 30, 45	5	6	504	630
DD9800 w/ HA [3]	256	3x4	SAS 30, 45, 60	5	6	504	630
DD9800 [3, 4]	768	3x4	SAS 30, 45, 60; SATA 15, 30, 45	5	6	1008	1260
DD9800 w/ HA [3]	768	3x4	SAS 30, 45, 60	5	6	1008	1260
DD9800 w/ ER [3]	768	4x4	SAS 30, 45, 60; SATA 15, 30, 45	7	8	2016	2520
DD9800 w/ Cloud Tier [3]	768	4x4	SAS 30, 45, 60; SATA 15, 30, 45	7	8	1008 (max), additional 240 SAS dedicated to Cloud Tier	1260 (max), additional 300 SAS dedicated to Cloud Tier
DD9800 w/ HA and Cloud Tier [3]	768	4x4	SAS 30, 45, 60	7	8	1008 (max), additional 240 SAS dedicated to Cloud Tier	1260 (max), additional 300 SAS dedicated to Cloud Tier

1. This figure only counts drives that have user data in the shelves.

2. The raw capacity of an ES30 is 125% of the available capacity.

3. Only available with DD OS 5.x and greater.

4. DDOS 6..x and greater and FS15 SSD shelf configuration

Types of cabinets and power connections

The ES30 chassis is installed in two types of racks: 40U-C (existing racks) and the 40U-P (newer racks). The racks use one phase or 3-phase power connections.

3-Phase power connections for 40U-P (current racks)

Some environments use 3-phase power for 40U-P racks that are used for several systems. In those situations, it is desirable to balance the current draw across all three phases. The recommended 3-phase power cabling attempts to do that, but an optimal configuration depends on the specific installation.

Cabling shelves

NOTE:

- Before cabling the shelves, physically install all shelves in the racks. Refer to the rail kit installation instructions included with the ES30 shelf for rack mounting.

- The documentation refers to two SAS HBAs. If only one HBA is allowed in a system, then use another port as defined later for that specific system.
- On an HA system, add cables from the second node to open ports at the end of the sets. The ports on the second node must connect to the same sets as the corresponding ports on the first node.

Ports on the system's SAS HBA cards connect directly to a shelf controller's host port. For redundancy, you need to create dual paths by using a port on one SAS HBA card to connect to one shelf controller in each shelf set, and a port on another SAS HBA card to connect to another shelf controller in the same shelf set. With dual paths, if one SAS HBA card fails, the shelf is still operational. However, in the unlikely event any single shelf becomes completely disconnected from power or SAS cables and becomes disconnected from a previously operational shelf, the file system goes down and the shelf is not operational. This is considered a double failure.

There are two kinds of configurations: one shelf in a set or multiple shelves in a set.

DD9500 and cabling

NOTE: If a system installation does not follow ALL of these rules, it is not a legitimate configuration.

Prerequisites:

- Follow the minimum and maximum shelf capacity configuration provided in the table.
- You cannot have ES30 SATA and ES30 SAS shelves in the same set.
- You cannot exceed the maximum amount of raw capacity displayed in the product's cabling table.
- You cannot exceed the maximum number of shelves displayed in the product's cabling table.
- You cannot have more than five ES30s in a single set (maximum of four is preferred).
- You can have seven ES30s for systems with Extended Retention software.
- There are no specific placement or cabling requirements for SSD shelves, or the metadata shelves for Cloud Tier configurations. These shelves can be installed and cabled the same way as standard ES30 shelves.

Table 184. Minimum and maximum configurations

System	DD9500	DD9500 w/	
Appliance	864 TB usable	864 TB usable	1008 TB usable
Minimum appliance shelf count	4	4	4
Maximum appliance shelf count	30	30	30
Extended Retention systems (ER)	1728 TB usable	2016 TB usable	2016 TB usable
Maximum shelves for ER	56	56	56
High Availability systems (HA)	864 TB usable	1008 TB usable	1008 TB usable
Maximum shelves for HA	42	42	47
Cloud Tier systems	1104 TB usable	1248 TB usable	1248 TB usable
Maximum shelves for Cloud Tier	42	42	47

The DD9500 base (non-Extended Retention) and HA systems supports six chains.

The following figures show cabling for base systems, HA systems, and systems with the Extended Retention software option.

NOTE: The racks are filled from bottom up.

DD9800 and DS60 shelf guidelines

The system rediscovers newly configured shelves after it restarts. You can power off the system and recable shelves to any other position in a set, or to another set. To take advantage of this flexibility, you need to follow these rules before making any cabling changes:

- Do not exceed the maximum shelf configuration values for your system as listed in the following table.
- For redundancy, the two connections from a system to a set of shelves must use ports on different SAS I/O modules.
- Use the Installation and Setup Guide for your system to minimize the chance of a cabling mistake.
- A system cannot exceed its maximum raw external shelf capacity, regardless of added shelf capacity.
- ES30 SATA shelves must be on their own chain.
- If ES30 SAS shelves are on the same chain as a DS60, the maximum number of shelves on that chain is 5.

Table 185. DD9800 and DS60 shelf configuration

DD system	Memory required (GB)	SAS cards/ port per card	DS60 support (TB)	Max shelves per set	Max number of sets	Max external capacity available (TB)[1]	Max RAW external capacity (TB)
DD9800 [2, 3]	256	3x4	SAS 45, 60	4	6	504	630
DD9800 w/ HA[2, 3]	256	3x4	SAS 45, 60	4	6	504	630
DD9800 [2, 3]	768	3x4	SAS 45, 60	4	6	1008	1260
DD9800 w/HA [2, 3]	768	3x4	SAS 45, 60	4	6	1008	1260
DD9800 ER [2, 3]	768	4x4	SAS 45, 60	4	8	2016	2520
DD9800 Cloud Tier [2, 3]	768	4x4	SAS 45, 60	5	8	1008 + 240 for Cloud Tier	1260 + 300 for Cloud Tier
DD9800 Cloud Tier w/ HA [2, 3, 4]	768	4x4	SAS 45, 60	5	8	1008 + 240 for Cloud Tier	1260 + 300 for Cloud Tier

NOTE: An entry of 45 corresponds to DS60-3 models and an entry of 60 corresponds to DS60-4 models.

1. This column only counts drives that have user data in the shelves. For example, a DS60 4-240 has 192TB.

2. With DD OS 6.x and greater with SSD.

3. Only available with DD OS 6.x and greater.

4. With Cloud Tier Storage.

3-phase power connections for 40U-P (current racks)

Some environments use 3-phase power for 40U-P racks used for several systems. In those situations it is desirable to balance the current draw across all 3 phases. The recommended 3-phase power cabling attempts to do that, but an optimal configuration is dependent on the specific installation.

DD9500 and DD9800 cabling

NOTE: If a system installation does not follow ALL of these rules, it is not a legitimate configuration.

Prerequisites:

- Follow the minimum and maximum shelf capacity configuration provided in the table.
- You cannot have ES30 SATA and ES30 SAS shelves in the same set.
- You cannot exceed the maximum amount of raw capacity displayed in the product's cabling table.
- You cannot exceed the maximum number of shelves displayed in the product's cabling table.
- You cannot have more than five ES30s in a single set (maximum of four is preferred).
- You can have seven ES30s for systems with Extended Retention software.

- There are no specific placement or cabling requirements for SSD shelves, or the metadata shelves for Cloud Tier configurations. These shelves can be installed and cabled the same way as standard ES30 shelves.

Table 186. Minimum and maximum configurations

System	DD9500	DD9500 w/	
Appliance	864 TB usable	864 TB usable	1008 TB usable
Minimum appliance shelf count	4	4	4
Maximum appliance shelf count	30	30	30
Extended Retention systems (ER)	1728 TB usable	2016 TB usable	2016 TB usable
Maximum shelves for ER	56	56	56
High Availability systems (HA)	864 TB usable	1008 TB usable	1008 TB usable
Maximum shelves for HA	42	42	47
Cloud Tier systems	1104 TB usable	1248 TB usable	1248 TB usable
Maximum shelves for Cloud Tier	42	42	47

The DD9500 base (non-Extended Retention) and HA systems supports six chains.

The following figures show cabling for base systems, HA systems, and systems with the Extended Retention software option.

NOTE: The racks are filled from bottom up.

14

DD9900

This chapter contains the following topics:

Topics:

- DD9900 system features
- DD9900 system specifications
- DD9900 storage capacity and configurations
- DD9900 front panel
- DD9900 SSD usage and configurations
- DD9900 rear panel
- PCIe HBAs
- DD9900 DIMM configurations
- DD6900, DD9400, and DD9900 storage shelves configurations and capacities

DD9900 system features

Table 187. DD9900 system features

Features		Single Node	HA
Processor		4 x Intel Xeon 6240, 18C, 2.6GHz, 150W	
Kernel		4.4	
Memory Configurations	Total	1152 GB	
	DIMMs	24 x 16 GB + 24 x 32 GB	
HDD Drive Size		8 TB (3 TB and 4 TB also supported)	
Supported Capacity	Active Tier	576 <-> 1536 TBu	
	Cloud Tier	3072 TBu (Cloud Tier)	
Disk Groups	Active Tier	8 <-> 18 (8 TB), 8 <-> 28 (3 TB), 8 <-> 32 (4 TB)	
	Cloud Tier (4 TB)	6	
SSDs for DD OS in 2.5" bays in head		4, 1.92TB, 1 WPD	
Stream Count		1865 Wr, 300 Rd	
Cache SSDs	2.5%	10 (External FS25) 3.84 TB	
Cache SSD shelf	FS25	1	
HA Private Interconnect		N/A	(3) 10G Base-T ports (NDC)
16 GB NVRAM		1	
HW Accelerator	100 Quick Assist Technology (QAT) 8970	2	
Internal SAS	PowerEdge Raid Controller (PERC) H330+ 12 Gbps SAS	1	
External SAS	PMC Quad Port 12 Gbps SAS	2 default, 3 supported	

Table 187. DD9900 system features (continued)

Features		Single Node	HA
SAS String Depth (max)	ES30/ES40	7	
	DS60	3	
Host interface HBAs	2-port 100 GbE-QSFP28	4 maximum	
	2-port QL41000 25 GbE-SFP28	4 maximum	
	4-port QL41164 10 GbE-SFP+	4 maximum	
	4-port QL41164 10GBASE-T	4 maximum	
	4-port QLE2694 16 Gb FC	4 maximum	
Network Daughter Card options (system will have one of the two options)	4-port QL41000 10 GbE-SP+ FasLinQ	1	
	4-port QL41164 10GBASE-T	1	

DD9900 system specifications

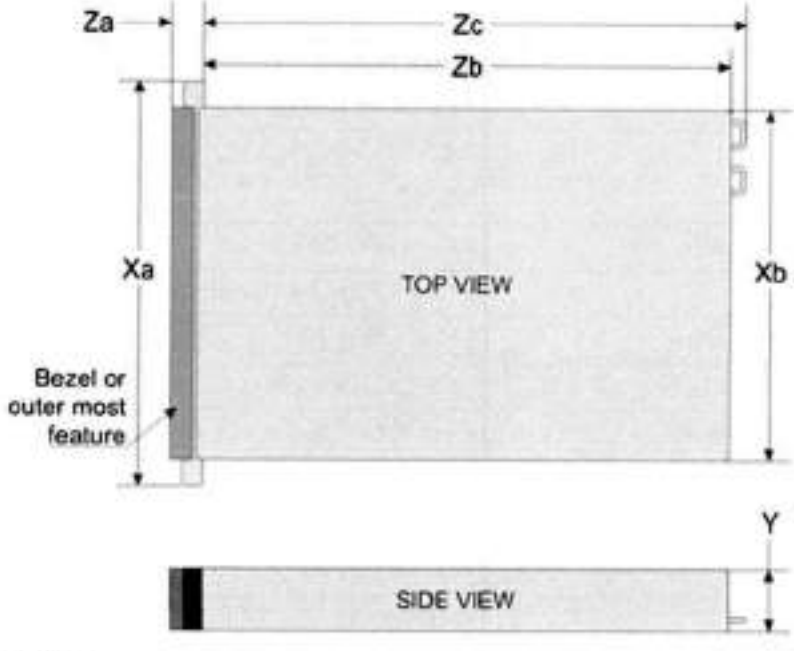


Figure 162. System dimensions

Table 188. DD9900 system specifications

Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb	Zc
482.0 mm (18.98 inches)	434.0 mm (17.09 inches)	130.3 mm (5.13 inches)	35.0 mm (1.37 inches)	22.0 mm (0.87 inches)	726.2 mm (28.59 inches)	777.046 mm (30.59 inches)

A DD9900 system weighs up to 110.01 lbs (49.9 kg).

Table 189. System operating environment

Operating Temperature	50° to 95° F (10° to 35° C), derate 1.1° C per 1000 feet, above 7500 feet up to 10,000 feet (32.25° C at 10,000)
Operating Humidity	20% to 80%, non-condensing
Non-operating Temperature	-40° to +149° F (-40° to +65° C)
Operating Acoustic Noise	L_{wad} sound power, 7.5 Bels

DD9900 storage capacity and configurations

The following table provides storage capacity and configuration information for the DD9900 system.

Table 190. DD9900 storage capacity and configurations

Tier	CPU-SP SKU	Memory	Front 2.5" SSDs	Max. Useable Capacity	Cloud Tier Metadata
DD9900 Active Tier	18 core, 150 W 6240	1152 GB (24 x 16 GB) + (24 x 32 GB)	10	1536TBu	N/A
DD9900 with Cloud Tier [1]	18 core, 150 W 6240	1152 GB (24 x 16 GB) + (24 x 32 GB)	10	3072TBu	360 TB raw/288 TB usable

[1] Cloud Tier can be added to a DD9900 and is enabled by a license and disk packs for the Cloud Tier metadata.

The Memory column lists the total memory that is required and the number and type of the DIMMs used. All memory DIMMs are DDR4 RDIMMs at the highest supported speed of 2666MT/s.

High Availability

DD9900 supports Active-Passive High Availability (A-P HA or a-P). The following table summarizes the hardware changes to support A-P HA:

Table 191. HA configuration requirements

Hardware Change to support HA	Active-Passive HA
Additional memory	No extra memory required.
HA private interconnect	Cluster Interconnect : A-P requires the use of three ports from the on-board quad-port 10 GbE Network Daughter Card.
NVRAM	A-P requires a single 16 GB NVRAM card (same as non-HA).
SAS Connectivity	Both nodes of an A-P HA pair require redundant SAS connectivity to the storage array. (Note: a single node system also has redundant connectivity to the storage arrays.)
SSD Requirements	SSDs are contained within FS25 and must be accessible from both nodes.

HA Network Interconnect

The HA Network Interconnect, required for HA configurations, is a dedicated 10 GbE connection between the two nodes of an HA pair. The interconnect is used to write data (and metadata) from the active node's NVRAM to the passive node's NVRAM.

Two 10GbE links are used to meet the bandwidth requirements for the private interconnect. Traffic across the private interconnect has roughly the same bandwidth as is written to the NVRAM card. The three 10-GbE links can move about 2 GB/s in each direction.

HA SAS Interconnect

HA configurations require that the SSDs' cache drives be shared between both nodes and have redundant SAS connections to all shelves.

DD9900 front panel

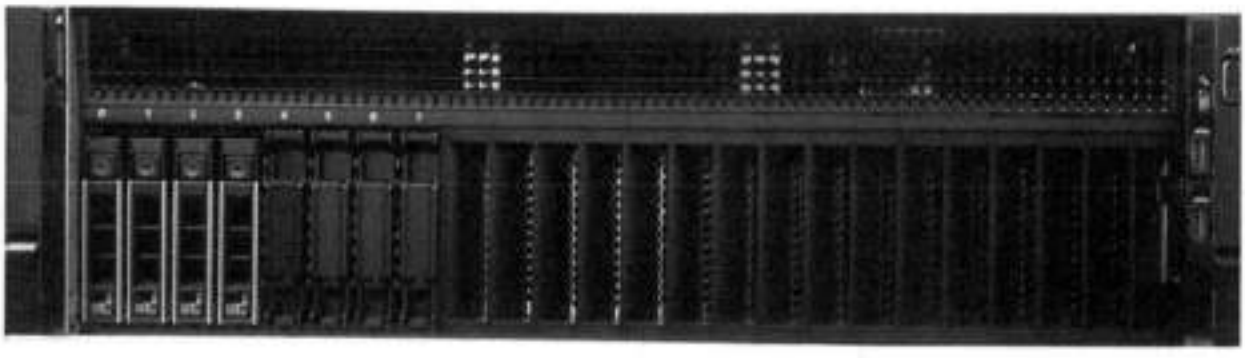


Figure 163. DD9900 front panel

Table 192. Front panel features

Item	Ports, panels, and slots	Description
1	Left control panel	Contains system health and system ID, status LED, and optional iDRAC Quick Sync 2 (wireless).
2	Drive slots	Enable you to install drives that are supported on your system.
3	Right control panel	Contains the power button, VGA port, iDRAC Direct port, and USB ports.
4	Information tag	The Information tag is a slide-out label panel that contains system information such as Service Tag, NIC, MAC address, and so on. If you have opted for the secure default access to iDRAC, the Information tag also contains the iDRAC secure default password.
5	Drive bay	Hard drive bay

Table 193. Front LEDs

Name	Color	Purpose
Control Panel Status LED	Blue/Amber	Status: • Healthy: Solid Blue • Fault: Blink Amber • Sys ID: Blink Blue
System Power Button/LED	Green	Indication that the system has power.
Drive activity LEDs	Green	Lit green when the drive is powered. Blinks during drive activity.
Drive service LEDs	Green	Lit solid amber when a disk drive needs service.

Front LEDs

Figure 164. Front left control panel status LEDs

NOTE: The indicators display solid amber if any error occurs.

Table 194. System health and system ID indicator codes

System health and ID indicator code	
Solid blue	Indicates that the system is turned on, system is healthy, and system ID mode is not active. Press the system health and system ID button to switch to system ID mode.
Blinking blue	Indicates that the system ID mode is active. Press the system health and system ID button to switch to system health mode.
Solid amber	Indicates that the system is in fail-safe mode.
Blinking amber	Indicates that the system is experiencing a fault. Check the System event log or the LCD panel, if available on the bezel, for specific error messages.

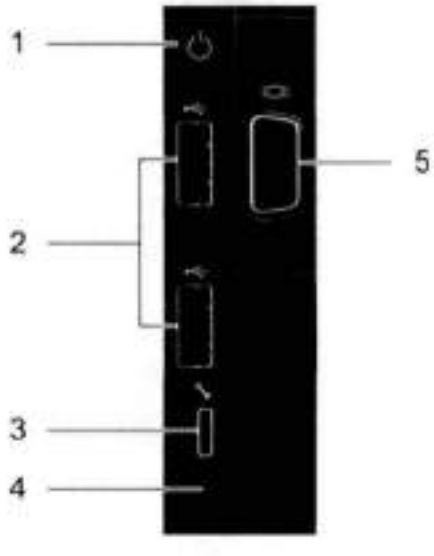


Figure 165. Front right control panel power button LEDs

Table 195. Right control panel features

Item	Indicator, button, or connector	Description
1	Power button	Indicates if the system is turned on or off. Press the power button to manually turn on or off the system. **NOTE:** Press the power button to gracefully shut down an ACPI-compliant operating system.

Table 195. Right control panel features (continued)

Item	Indicator, button, or connector	Description
2	USB port (2)	The USB ports are 4-pin, 2.0-compliant. These ports enable you to connect USB devices to the system.
3	iDRAC Direct port	The iDRAC Direct port is micro USB 2.0-compliant. This port enables you to access the iDRAC Direct features.
4	iDRAC Direct LED	The iDRAC Direct LED indicator lights up to indicate that the iDRAC Direct port is connected.
5	VGA port	Enables you to connect a display device to the system.

Table 196. iDRAC Direct LED indicator codes

iDRAC Direct LED indicator code	Condition
Solid green for two seconds	Indicates that the laptop or tablet is connected.
Flashing green (on for two seconds and off for two seconds)	Indicates that the laptop or tablet that is connected is recognized.
Turns off	Indicates that the laptop or tablet is unplugged.

Figure 166. Drive LEDs

The front contains 25 2.5" disk drive slots that can be populated with SSDs. Each SSD is housed in a drive carrier that contains two LEDs at the bottom of the carrier. The carrier's left blue LED is lit whenever an SSD is present in the slot, and it blinks when I/O activity is occurring on the disk. The right amber LED is usually off and lights amber to indicate that the disk is faulted and must be serviced.

DD9900 SSD usage and configurations

DD9900 system uses an 8 x 2.5" drive slot midplane. However, metadata cache devices are implemented using the external flash shelf FS25. This allows dual access to all SSD devices which doubles the SSD access bandwidth.

SSD configurations

The SSD slots on the front of the enclosure are shown below. The system come from the factory with SSDs populated in the enclosure.

DD9900 supports 2.5% SSD option out of factory. Based on 3.84 TB SSD capacity, the required number of SSDs for each DD9900 configuration is provided in the following table.

Table 197. DD9900 SSD configurations

Configuration	Single node	HA
Cache SSDs	10 (External FS25) 3.84 TB	

SSD boot drives

Other SAS SSDs are used to boot the operating system. Boot disks and external disk shelves are used to log system information. Boot disks are installed from the other end of the front 2.5" disk slots to physically differentiate the cache SSDs.

Table 198. SSD boot drives

# of boot disks	Installed in slots
Four 1.92TB SSDs	0,1,2,3

DD9900 rear panel

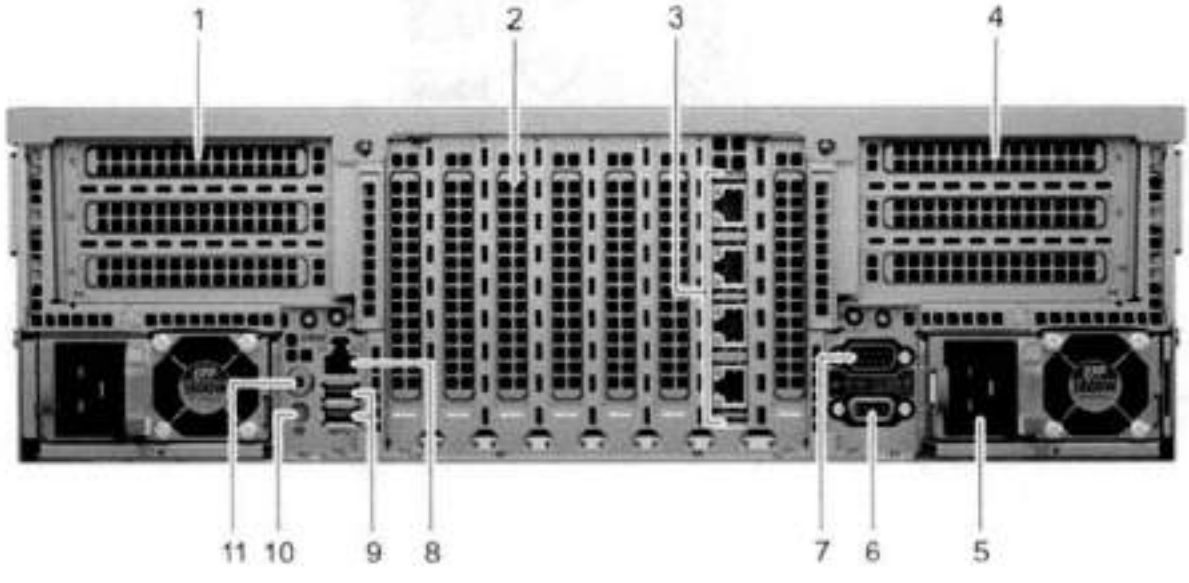


Figure 167. DD9900 rear panel

Item	Slot, button, or connector	Description
1	Half-height PCIe expansion card slot	The PCIe expansion card slot connects one half-height PCIe expansion cards to the system.
2	Full-height PCIe expansion slots	The PCIe expansion card slot connects up to three full-height PCIe expansion cards to the system.
3	NIC ports (4)	The NIC ports that are integrated on the network daughter card (NDC) provide network connectivity.
4	Half-height PCIe expansion card slot	The PCIe expansion card slot connects one half-height PCIe expansion cards to the system.
5	Power supply unit (2)	Supports two AC power supply units (PSUs)
6	VGA port	Enables you to connect a display device to the system.

Item	Slot, button, or connector	Description
7	Serial port	Enables you to connect a serial device to the system.
8	iDRAC9 Enterprise port	Enables you to remotely access iDRAC.
9	USB port (2)	The USB ports are 9-pin and 3.0-compliant. These ports enable you to connect USB devices to the system.
10	System identification button	The System Identification (ID) button is available on the front and back of the systems. Press the button to identify a system in a rack by turning on the system ID button. You can also use the system ID button to reset iDRAC and to access BIOS using the step through mode.
11	Status indicator cable port	Enables you to connect the status indicator cable and view system status when the CMA is installed.

Rear LEDs

Figure 168. Onboard ID and iDRAC LEDs

1. iDRAC management port:
   a. The green link LED on the left is lit whenever there is link at 1000BaseT and 100BaseT speeds. The link LED is off when the link speed is 10BaseT or there is no link.
   b. The green link LED on the right blinks whenever there is traffic on the port.
2. System identification LED: This blue LED can be turned on by software to visually identify the system.

PSU FRU LEDs

There are two power supplies, one in the upper left of the rear chassis and one on the bottom right. Each power supply has three LEDs: AC good, DC good, and Service. The top PSU is "right-side up" and the bottom PSU is "upside down."

Table 199. PSU FRU LEDs

Name	Color	Definition
AC Good	Green	AC input is as expected.
DC Good	Green	DC output is as expected.
Service	Amber	PSU has a fault condition and a must be replaced.

PCIe HBAs

A slot in the chassis that does not contain an HBA must have a filler panel installed in the empty slots. This is required for EMI compliance.

This system supports 13 I/O modules slots, three of which are 8-lane PCIe Gen3, and ten are 16-lane PCIe Gen3. Several networking, NVRAM, SAS, and Fibre Channel I/O modules are supported.

Slot assignment

The following table lists the DD9900 configuration slot assignments:

Table 200. DD9900 slot assignments

Description	Slot
QLogic, 41164 4 Port, 10GbE SFP+ PCIe, Full Height	6, 8, 4, 10, 3, 13, 5
QLogic, 41164 4 Port, 10GBASE-T PCIe, Full Height	8, 4, 3
QLogic, 41262 2 Port, 25Gb SFP28 PCIe, Full Height	6, 8, 4, 10, 3, 13, 5
Mellanox CX-5 2x 100GbE QSFP28 PCIe, FH	8, 3, 4, 13, 10
PERC H330+ SAS RAID Adapter, FH	1
QAT,INTEL,8970,FH, Avnet p/n 1QA89701G1P5	2, 7
PM8072,SAS12,4P,FH, MicroSemi 2295200-R	9, 12, 5
FC16,QLE2694-DEL-BK,TRG,QP,FH	5, 6, 8, 4, 10, 3, 13
16GB NVRAM,FH	11

Host Interface (x16) is 2-port 100 Gb QSFP28 Ethernet.

Host Interface (x8) are:

- 2-port 25 Gb SFP28 Ethernet
- 4-port 10 Gb SFP+ Ethernet
- 4-port 10GBaseT Ethernet
- 4-port 16 Gb Fibre Channel

External SAS is 4-port 12 Gb SAS card and is required for external storage for HA and Single Node configurations.

NVRAM is the 16GB NVRAM.

Internal SAS Mezzanine is 2-port 12 Gb Mini-SAS HD SAS controller mezzanine.

Host Network Interface Mezzanine is either:

- 4-port 10GBaseSR SFP+ Ethernet mezzanine
- 4-port 10GBaseT RJ45 Ethernet mezzanine

I/O population rules

The following figures show the I/O module slot numbers.

The slot labeled N is the network daughter card, which contains ports ethMa, ethMb, ethMc, and ethMd.

The physical interface name format for the other I/O module slots is ethXy, where X is the slot number and y is an alphanumeric character. For example, eth0a.

For most horizontal I/O module NIC interfaces, the port numbering goes from left to right, with ethXa on the left. The horizontal I/O module slots on the left-in slots 11-13 are inverted. The port numbering on these I/O modules in these slots goes from right to left, with ethXa on the right.

For vertical I/O module NIC interfaces, the port numbering goes from top to bottom, with ethXa at the top.

The management port ethMa is the first port set up by the Configuration Wizard. It is marked with a red rectangle in the figure below.

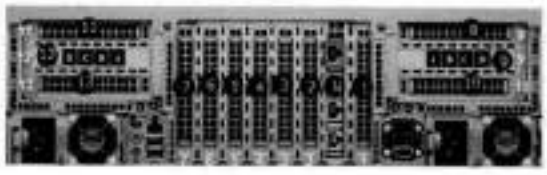


Figure 169. Slot numbering

The general population rules can be summarized as:

1. Populate a given I/O in the available slots listed.
2. Select the first available slot in the group.
3. Follow the steps for each I/O in the order specified.
4. Slots 1, 5 and 6 are x8 PCIE slots. All other PCIE slots are x16.

NOTE: Installing HBAs requires opening the system and installing the HBA into the riser.

Riser#	Slots (from top to bottom)
Left	11, 12, 13
Right	8, 9, 10

Slots 1, N, 2, 3, 4, 5, 6, and 7 are not installed on a riser.

Gen3 PCIe

Slots support Gen3 PCIe.

I/O module servicing

All I/O modules are user serviceable and may be replaced when the system is powered off. On-line service of I/O modules is not support. A module that is hot-inserted into the system will remain powered off and will not be powered on until the next reboot of the system. A module that is hot-removed causes an operating system to immediately reboot.

DD9900 DIMM configurations

The SP Module contains 4 Intel SP processors each with an integrated memory controller that supports six channels of DDR4 memory. The CPU allows two DIMM slots per channel, so the SP Module supports 24 DIMM slots.

Each DDR4 DIMM is connected to the system board through an industry standard 288-pin DDR4 DIMM connector. This system uses registered DIMMs with Dell EMC ControlCenter at 72 bits wide (64-bits data + 8-bits Dell EMC ControlCenter) up to a maximum of 2666MT/s speed.

Table 201. Memory configurations

Tier	Total Memory	Memory DIMM Configuration
DD9900 Active Tier	1152 GB	24 x 32 GB + 24 x 16 GB
DD9900 Cloud Tier	1152 GB	24 x 32 GB + 24 x 16 GB

Memory locations

To ensure maximum memory performance, there are memory DIMM population rules so that the memory loading and interleaving are optimal. The following table below specifies the DIMM location rules. Each DIMM location contains either a 16GB DIMM or a 32GB DIMM.

Table 202. DD9900 DIMM configuration CPU 1

Total (GB)	Channel C		Channel B		Channel A		Channel D		Channel E		Channel F	
	A6	A12	A5	A11	A4	A10	A7	A1	A8	A2	A9	A3
288 GB	32 GB	16 GB	32 GB	16 GB	32 GB	16 GB	16 GB	32 GB	16 GB	32 GB	16 GB	32 GB

Table 203. DD9900 DIMM configuration CPU 2

Total (GB)	Channel C		Channel B		Channel A		Channel D		Channel E		Channel F	
	B6	B12	B5	B11	B4	B10	B7	B1	B8	B2	B9	B3
288 GB	32 GB	16 GB	32 GB	16 GB	32 GB	16 GB	16 GB	32 GB	16 GB	32 GB	16 GB	32 GB

Table 204. DD9900 DIMM configuration CPU 3

Total (GB)	Channel C		Channel B		Channel A		Channel D		Channel E		Channel F	
	C6	C12	C5	C11	C4	C10	C7	C1	C8	C2	C9	C3
288 GB	32 GB	16 GB	32 GB	16 GB	32 GB	16 GB	16 GB	32 GB	16 GB	32 GB	16 GB	32 GB

Table 205. DD9900 DIMM configuration CPU 4

Total (GB)	Channel C		Channel B		Channel A		Channel D		Channel E		Channel F	
	D6	D12	D5	D11	D4	D10	D7	D1	D8	D2	D9	D3
288 GB	32 GB	16 GB	32 GB	16 GB	32 GB	16 GB	16 GB	32 GB	16 GB	32 GB	16 GB	32 GB

DD6900, DD9400, and DD9900 storage shelves configurations and capacities

DD6900, DD9400, and DD9900 do not store data on internal disk drives and rely on external disk array shelves to provide storage. DS60 disk shelves and ES40 shelves are connected to systems using 12 Gb Mini-SAS HD ports, which are implemented on the SAS HBAs.

The systems also support external metadata storage (cache) shelf FS25. External cache shelf only hosts DD OS depended metadata for performance acceleration.

The ES40 SAS shelf contains 15 drives, which includes 12 drives of usable storage, two parity drives, and one hot spare.

The DS60 shelf contains 60 drives. Drives are configured in four groups of 15 drives. Each group contains two parity drives and one hot spare, so each group provides 12 drives of usable storage. A fully configured DS60 shelf provides 48 drives of usable storage.

Table 206. Shelves shipped from factory, in rack

DD6900	DD9400	DD9900
4 TB ES40	8 TB DS60	8 TB DS60

Table 207. Shelves shipped from factory, boxed

DD6900	DD9400	DD9900
4 TB ES40	8 TB ES40	8 TB ES40
4 TB DS60	8 TB DS60	8 TB DS60

Table 208. Additional shelves supported

DD6900	DD9400	DD9900
4 TB SAS ES30/DS60	4 TB SAS ES30/DS60	4 TB SAS ES30/DS60
3 TB SAS ES30/DS60	3 TB SAS ES30/DS60	3 TB SAS ES30/DS60

NOTE: 3 TB shelves are only support on controller upgrades and not on fresh installs.

Table 209. Shelf usable capacities

Hard drive size (TB)	Shelf	Useable TB
4	ES40	48
4	DS60	192
8	DS60	384

The following table lists the maximum number of shelves per chain:

Table 210. Supported shelf count per chain

Shelf type	Max # from factory	Max # per chain
SAS ES30/ES40	4	7
DS60	2	3
DS60 + ES30/ES40	n/a	5
F25	1	1

The connector type for ES30 is Mini-SAS. Special cables may be necessary when combining ES30 and ES40 shelves on the same chain (enabled but not recommended).

DD9400 and DD9900 system capacities are optimized for use with DS60 shelves containing 8 TB drives. DS60 shelves can be populated with one to four packs of fifteen 8 TB, or 4 TB drives. Different 4 TB and 8 TB capacity disk packs may be mixed within a single DS60 shelf. ES40 SAS shelves and DS60 shelves of mixed capacities may be attached so long as the maximum storage capacity of the system is not exceeded.

15

DS60

This chapter contains the following topics:

Topics:

- DS60 overview
- DS60 site requirements
- DS60 hardware specifications
- DS60 front panel
- Back panel
- Disk enclosure interior
- Expansion shelf cables
- Ports

DS60 overview

Adding DS60 expansion shelves to a system increases the system's storage capacity.

The expansion shelves are organized by sets (or chains). The following table shows the number of DS60 shelves in set (chain) each system can support.

Table 211. DS60 shelf set support

System (base)	DS60 shelves
DD6300	1 shelf only*
DD6800, DD9300, DD9500, and DD9800	4 per set (chain)

* DD6300 systems only supports the addition of one DS60 expansion shelf.

DS60 site requirements

This table lists the DS60 site requirements. See DS60 hardware specifications for hardware specifications information.

Table 212. Site requirements

Requirement	DS60 Expansion Shelf
Vertical space in standard 19", 4-post rack	5U including a 1U Cable Managements Tray. Do not use a two-post rack. See the slide rail and installation documentation in the packaging for installing in a rack.
Air conditioning	Air conditioning that can cope with the maximum BTU/hr thermal rating.
Temperature controls	Adequate temperature control with a gradient (change) not to exceed 30° C in an hour.
Front bezel clearance	1.56 inches (4.0 cm) of unobstructed clearance.
Back panel clearance	5 inches (12.7 cm) of unobstructed clearance.
Airflow	In a closed or multi-unit rack, ensure that the unit has adequate airflow. If the equipment is mounted in an enclosed (as opposed to a four-post open rack), the front and rear doors should have 65% minimum open area for airflow.

Table 212. Site requirements (continued)

Requirement	DS60 Expansion Shelf
	Whether in an open or enclosed rack, use filler panels to prevent hot air re-circulation. The rack design and installation should take into consideration the maximum ambient operating temperature of the equipment, which is 35° C.
Power/grounding	The Power distribution within the rack should provide a safe electrical earth connection. Voltage should be 200-240 VAC; 50 or 60 Hz. Plug four power cords - two from each power supply into separate branch circuit supplies for redundancy—one set of cords from one power supply goes to one branch and the second set of cords from the other power supply goes to a different branch. Each receptacle must be capable of safely supplying 0.94 amps from each power socket or 1.87 amps from each socket in case of a redundant circuit.

DS60 hardware specifications

NOTE: All ratings assume a fully configured DS60 shelves.

Table 213. Hardware specifications

Specification	Description
AC line voltage	200 to 240 Vac ± 10%, single-phase, 47 to 63 Hz
AC line current (operating maximum)	4.9 A max at 200 Vac
Power consumption (operating maximum)	980 VA (931W) max
Power factor	0.95 min at full load, low voltage
Heat dissipation (operating maximum)	3.36 x 10^6 J/hr, (3177 Btu/hr) max
Dimensions (rack mounted)	• Height: 8.75 in (22.23 cm) 5U (4U plus 1U cable management tray). • Width including rails: 17.50 in (44.45 cm) • Depth (chassis only): 34.5 in (87.63 cm) • Maximum depth (fully configured): 36.4 in (92.46 cm)
Shelf weight	• Without FRUs installed: 55.0 lb (24.7 kg) • With FRUs installed: 225.0 lb (102 kg)
Operating temperature	• Ambient temperature: 41° F to 104° F (5° C to 40° C) • Temperature gradient: 18° F/hr (10° C/hr) • Relative humidity extremes: 20% to 80% noncondensing
Recommended operating relative humidity	40% to 55% noncondensing
Operating elevation	-50 to 7500 ft (-16 to 2300 m)
Non-operating (shipping and storage) temperature	• Ambient temperature: -40° F to 149° F (-40° C to 65° F) • Temperature gradient: 45° F/hr (25°C/hr) • Relative humidity: 10% to 90% noncondensing • Elevation: -50 to 35,000 ft (-16 to 10,600 m)

DS60 front panel

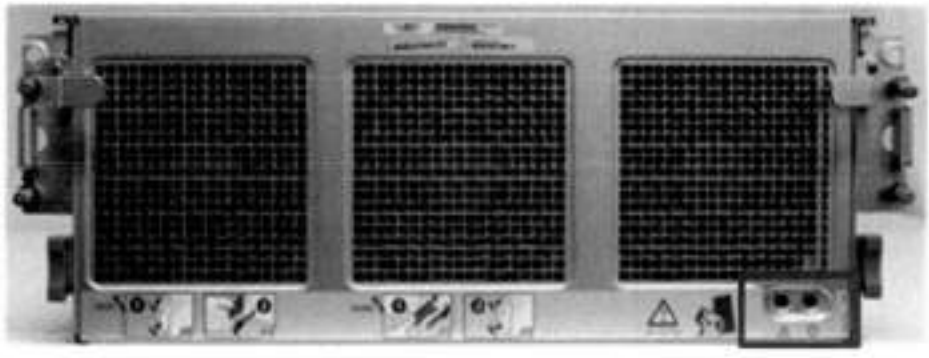


Figure 170. DS60 front panel

NOTE: The front LEDs are identified inside the red rectangle.

If there is a problem with the enclosure, the enclosure fault light LED (marked with a triangle with an exclamation mark) is amber. When the shelf is powered on and active, the disk enclosure power LED (marked with a circle with a vertical line) is blue.

Table 214. LED status lights

Light	Quantity	Color	Meaning
Disk Enclosure Power	1	Blue	Power to enclosure is on.
Disk Enclosure Fault	1	Amber	On when any fault condition exists: If the fault is not obvious from a disk or fan module light, look at the back of the disk enclosure.

NOTE: The individual disk LEDs are only visible when the disk enclosure is opened to verify the disks inside.

For part replacement information, refer to the *DS60 Expansion Shelf Installation and FRU Replacement Guide*.

Back panel

The back panel has two dual power supplies and two LCCs (Link Controller Cards).

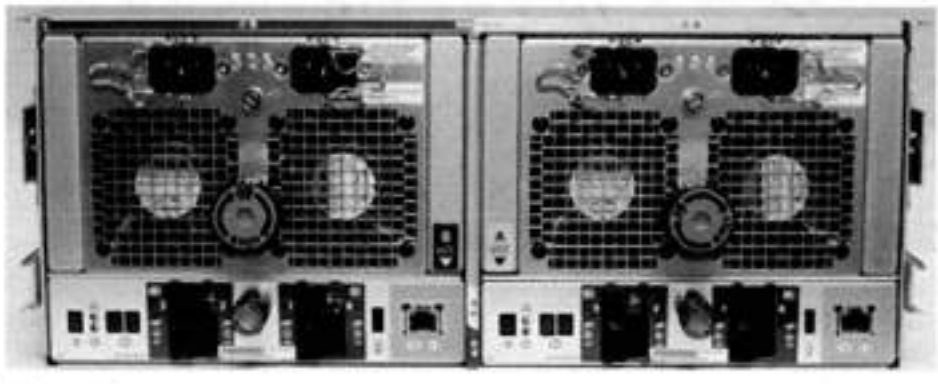


Figure 171. DS60 back panel

Each controller has 4 SAS ports (laid out as 2 pairs). Standard systems and systems with the licensed HA feature only use ports 0 and 2 on each controller. Ports 1 and 3 typically have a plastic plug blocking the unused ports to make inserting a cable into the correct ports easier.

Table 215. Status lights visible from rear of disk enclosure

Light	Quantity	Color	Meaning
Controller power	1 per controller	Green	On when the Controller is powered on.
Controller fault	1 per controller	Amber	On when either the Controller or a SAS connection is faulty. On during power-on self test.
Link active	4 per controller	Blue	On when the host connection is active.
Power supply input voltage	1 per power supply	Green	Input power green when it is working.
Power supply fault*	1 per power supply	Amber	• On when the power supply is faulty or is not receiving AC line voltage. • Flashing when either a multiple blower or ambient over temperature condition has shut off DC power to the system.

The DS60 continues to run with a single power supply and two fans (out of the three fans).

Disk enclosure interior

The disks are visible when the DS60 is pulled out of the rack and the top cover is removed from the chassis. There are also three fans in the front of the disk enclosure and each fan has a fault LED.

Each disk in the enclosure has two LEDs. The active LED glows blue when the disk is functional. The disk fault LED glows amber when the disk has failed.

NOTE: The individual disk and fan LEDs are only visible when the disk enclosure is opened to verify the disks inside.

Figure 172. Fans and disk drives inside the disk enclosure

Table 216. LED status lights

Light	Quantity	Color	Meaning
Disk Active **NOTE:** Only visible after the disk enclosure is opened.	1 per disk module	Blue	• No LED when the slot is empty or has a filler module. Also, off when the disk is powered

Table 216. LED status lights (continued)

Light	Quantity	Color	Meaning
			down by command; for example, the result of a temperature fault. • Fast blinking when the SAS drive is powered up but not spinning; this is a normal part of the spin-up sequence, occurring during the spin-up delays of a slot. • On when the drive has power but is not handing any I/O activity (the ready state). • Disk and fan lights are only available when enclosure is removed from the chassis. • Slow blinking when the drive is spinning and handling I/O activity.
Disk Fault **NOTE:** Only visible after the disk enclosure is opened.	1 per disk module	Amber	On when the disk module is faulty, or as an indication to replace the drive.
Fan fault	1 per fan module	Amber	On when the fan module is faulty, or as an indication to replace the fan.

The DD OS software manages the drives in packs (groups) of 15. A top down view of the chassis shows that the disks are arranged in four packs (groups) of 15 drives. The packs are color coded—pack 1 purple, pack 2 is yellow, pack 3 is green, and pack 4 is pink. A pack must have the same size drives. Pack 1 is shown within the red rectangle.

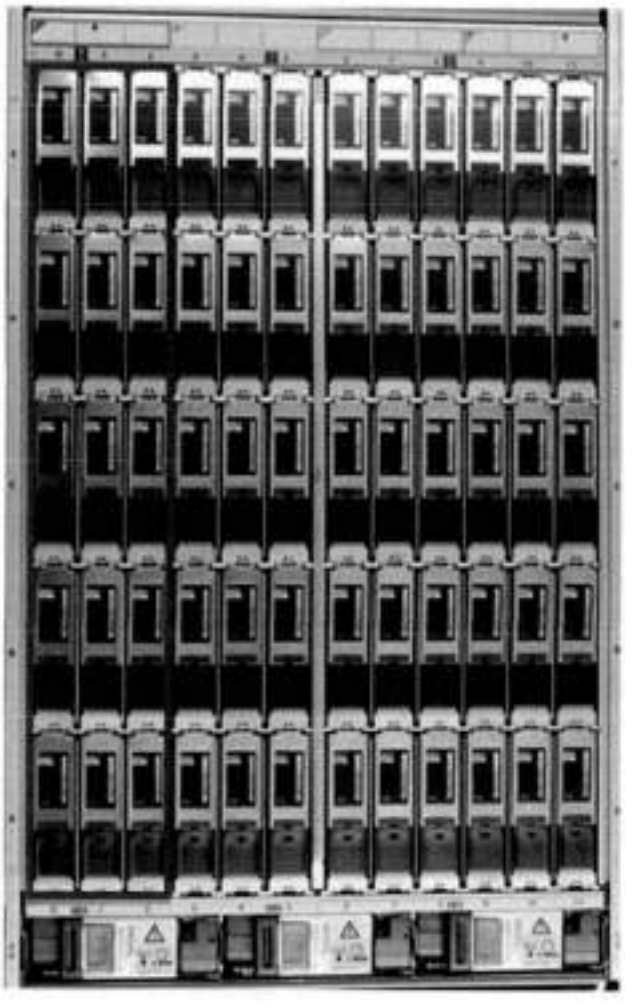


Figure 173. Drives as packs

The next table shows how the drives are distributed by packs (groups) and numbered physically. The bottom of the table represents the front of the shelf

Table 217. Physical drives

Rows	Pack 1	Pack 2	Pack 3	Pack 4
E	0-2	3-5	6-8	9-11
D	0-2	3-5	6-8	9-11
C	0-2	3-5	6-8	9-11
B	0-2	3-5	6-8	9-11
A	0-2	3-5	6-8	9-11

Although the disk numbers are physically 0 to 59, the disks are reported logically by system software commands in two ways:

- A range from 1 to 60, usually reported with the enclosure number (e.g. 3.37)
- The position matrix A-E (1-12)

For part replacement information, refer to the *DS60 Expansion Shelf Installation and FRU Replacement Guide*.

Expansion shelf cables

Expansion shelves are connected to each other and to the controller with qualified cables. The expansion shelf can be connected to supported systems only by using SAS (serial-attached SCSI) cables. A shelf with qualified disks can be added as an expansion shelf if there are complete drive packs (15 in a pack) in the correct position.

NOTE: Shelves for other Dell EMC product lines look identical. Check the product numbers when unpacking.

DS60 cables

The DS60 shelves use cables with HD-mini-SAS connectors at both ends to connect the shelves to the controllers that have SAS I/O modules.

The DS60 connector is referred as the HD-mini-SAS connector and is same as the I/O module connectors. These cables are available in 3M, 4M, and 5M lengths.

Use the appropriate length for the connection you are making:

- Use the 3-meter cable in the same rack either to connect to a controller or shelf to adjacent shelf.
- Use a 3-meter, 4-meter, or 5-meter cable when a DS60 is in another rack.

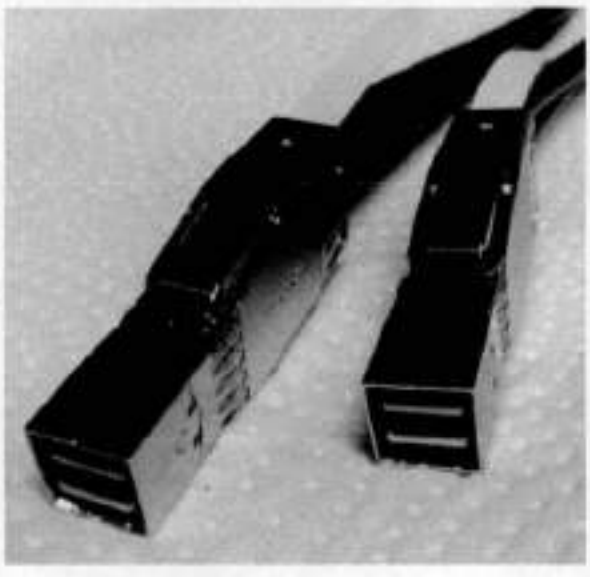


Figure 174. HD-mini-SAS connector

Table 218. HD-mini-SAS to mini-SAS cable part numbers

Cable Part Number	Cable Length
038-004-380-01	3M(118 in.)
038-000-212-00	4M (158 in.)
038-000-214-00	5M (196 in.)

Special cables must be used when attaching an ES30 to a chain with a DS60. Specifically, one HOST (circle) connection and one EXPANSION (diamond) cables are connected between the ES30 LCC and the DS60 LCC connection. Since this is not a common situation, only two expansion cable lengths are available.

Table 219. HD-mini-SAS to ES30 host and ES30 expansion port cable part numbers

Cable Part Number	Cable Type	Cable Length
038-003-810	Host	2M (78 in.)
038-003-813	Host	5M (196 in.)

Table 219. HD-mini-SAS to ES30 host and ES30 expansion port cable part numbers (continued)

Cable Part Number	Cable Type	Cable Length
038-004-108	Expansion	2M (78 in.)
038-004-111	Expansion	5M (196 in.)

The cable connectors must be secured with their latch assembly.

Ports

Depending on the model, a system has two to four quad-port SAS IO modules installed. The DS60 shelf has two controllers, and each DS60 controller has four ports, labeled 0, 1, 2, and 3 (right to left).

16

ES30

This chapter contains the following topics:

Topics:

- ES30 overview
- Site requirements
- ES30 hardware specifications
- Front panel
- Back panel
- Ports

ES30 overview

Adding ES30 expansion shelves to a system increases the system's storage capacity.

The expansion shelves are organized by sets (or chains). The following table shows the number of ES30 shelves than can be in a set.

Table 220. ES30 shelves in a set

Configuration	ES30 shelves
Base systems	1–4
Extended Retention software option	1–7

For redundancy, a shelf set is usually connected to two separate SAS I/O modules or HBA cards on the controller, and all of the shelves within a set are connected to each other via dual paths.

Site requirements

This table lists the site requirements.

Table 221. Site requirements

Requirement	expansion shelf
Vertical Space in Standard 19", 4-post Rack	3U. Do not use a two-post rack. See the slide rail and installation documentation in the packaging for installing in a rack.
Air Conditioning	Air conditioning that can cope with the maximum BTU/hr thermal rating.
Temperature Controls	Adequate temperature control with a gradient (change) not to exceed 30° C in an hour.
Front Bezel Clearance	1.56 inches (4.0 cm) of unobstructed clearance.
Back Panel Clearance	5 inches (12.7 cm) of unobstructed clearance.
Airflow	In a closed or multi-unit rack, ensure that the unit has adequate airflow. If the equipment is mounted in an enclosed (as opposed to a four-post open rack), the front and rear doors should have 65% minimum open area for airflow. Whether in an open or enclosed rack, use filler panels to prevent hot air recirculation. The rack design and installation should take into consideration the maximum ambient operating temperature of the equipment, which is 35° C.
Power/ Grounding	Two single-phase AC power outlets with an earth ground conductor (safety ground). A safe electrical earth connection must be provided to each power cord. Voltage should be 100-120 VAC or 200-240 VAC; 50 or 60 Hz. Use only with branch circuits protected by a minimum

Table 221. Site requirements (continued)

Requirement	expansion shelf
	15A overcurrent protector. Plug the two power cords into separate branch circuit supplies for redundancy.

ES30 hardware specifications

NOTE: All ratings assume a fully configured ES30.

Table 222. ES30 hardware specifications

Specification	Description
AC line voltage	100 to 240 Vac ± 10%, single-phase, 47 to 63 Hz
AC line current (operating maximum)	2.8 A max at 100 Vac; 1.4 A max at 200 Vac
Power consumption (operating maximum)	280 VA (235 W) max
Power factor	0.98 min at full load, low voltage
Heat dissipation (operating maximum)	8.46 x 10^5 J/hr, (800 Btu/hr) max
Dimensions (rack mounted, with bezel)	• Width: 17.62" (45 cm) Depth: 14" (35.56cm) • Height: 5.25" (13.34cm) 3 RU
Maximum Weight	68 lbs (30.8 kg)

Table 223. System operating environment

Operating Temperature	• Ambient temperature: 10° C to 35° C (50° F to 95° F) • Temperature gradient: 10° C/hr (180° F/hr) • Relative humidity extremes: 20% to 80% noncondensing	
Recommended Operating Relative Humidity	40% to 55% noncondensing	
Operating Humidity	• Ambient temperature: -40° C to 65° C (-40° F to 149° F) • Temperature gradient: 25° C/hr (45°F/hr) • Relative humidity: 10% to 90% noncondensing	
Non-operating Temperature	-40° to +149° F (-40° to +65° C)	
Operating Acoustic Noise	Sound power, LWAd: 7.4 bels. Sound pressure, LpAm: 58 dB. (Declared noise emission per ISO 9296.) Expansion Shelves: Max 58 dB LpA average measured at bystander positions	

Front panel

After you unlock and remove the snap-on bezel on the front panel, the 15 disks are visible. Disk numbers, as reported by system commands, range from 1 to 15. When facing the front panel, Disk 1 is located in the leftmost slot in the enclosure and Disk 15 in the rightmost slot.

Figure 175. ES30 front panel (bezel removed)

NOTE: The flanges or sheet metal on the ES30 show 0 to 14 but the software will refer to the logical numbering of 1 to 15.

Each disk in the enclosure has two LEDs. The disk's active LED glows green when the disk is functional. The disk fault LED glows amber when the disk has failed.

If there is a problem with the enclosure, the enclosure fault light is amber. The disk enclosure power light should be on (blue) when the shelf is powered on.

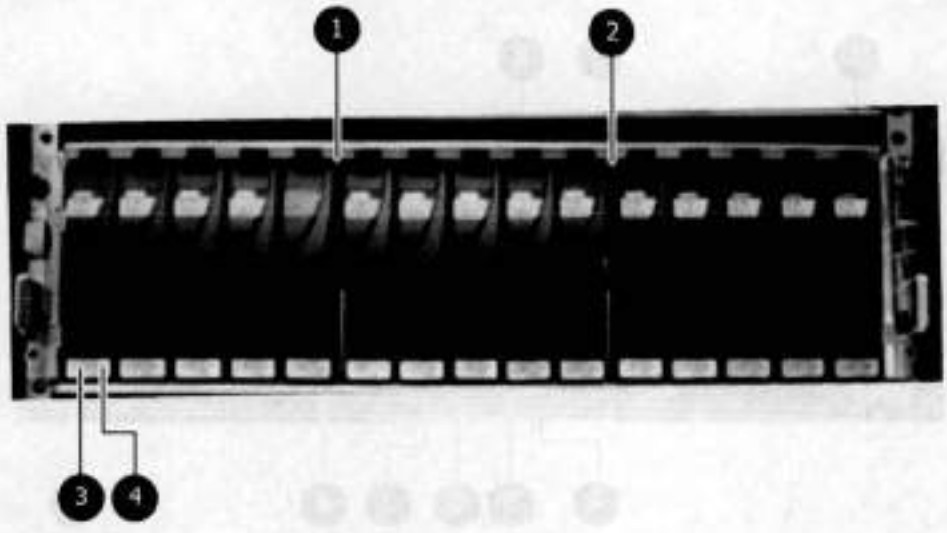


Figure 176. Front panel LEDs

1. Disk enclosure fault light
2. Disk enclosure power light
3. Disk active light
4. Disk fault light

Table 224. Status lights visible from front of disk enclosure

Light	Quantity	Color	Meaning
Disk enclosure fault light	1	Amber	On when any fault condition exists; if the fault is not obvious from a disk module light, look at the back of the disk enclosure.
Disk enclosure power light	1	Blue	Power to enclosure is on.
Disk active light	1 per disk module	Green	No LED when the slot is empty or has a filler module. Also, off when the disk is powered down by command; for example, the result of a temperature fault. Fast blinking when the SATA/SAS drive is powered up but not spinning; this is a normal part of the spin-up sequence, occurring during the spin-up delays of a slot. On when the drive has power but is not handing any I/O activity (the ready state. Slow blinking when the drive is spinning and handling I/O activity.

Table 224. Status lights visible from front of disk enclosure (continued)

Light	Quantity	Color	Meaning
Disk fault light	1 per disk module	Amber	On when the disk module is faulty, or as an indication to replace the drive.

Back panel

For redundancy, the shelf has two identical power supply/cooling modules and two identical shelf controllers which are placed in reverse order.

NOTE: When replacing a component, note its orientation before removing it. Insert the replacement in the same position.

Power supply A and controller A are located at the bottom of the chassis, and power supply B and controller B are located at the top of the chassis.

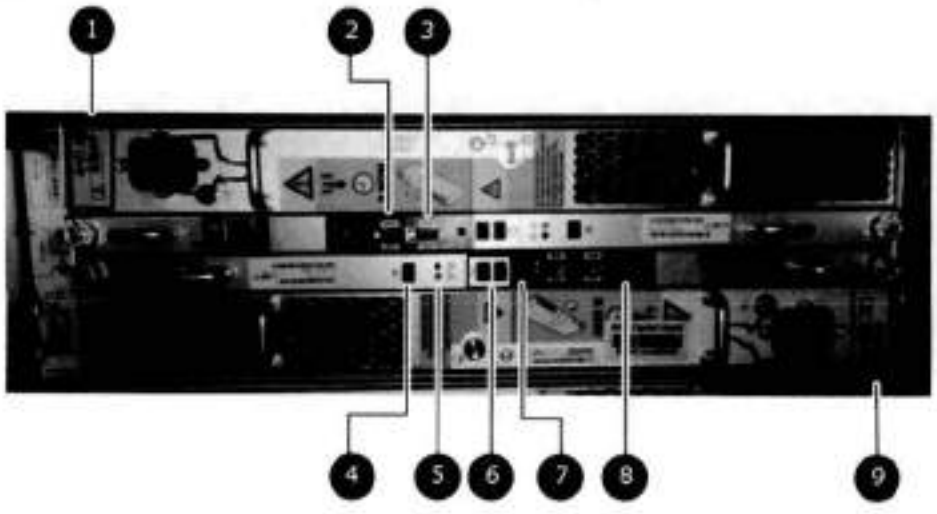


Figure 177. Back panel: Power modules and controllers

1. LEDs
   - Power supply B: Power LED
   - Power fault: Amber
   - Blower fault: Amber
2. Expansion (Out)
3. Host (In)
4. Enclosure address (not used)
5. Power (Green) or Fault (Amber)
6. Bus ID (not used)
7. Host link active
8. Expansion link active
9. LEDs
   - Power supply A Power LED
   - Power fault: Amber
   - Blower fault: Amber

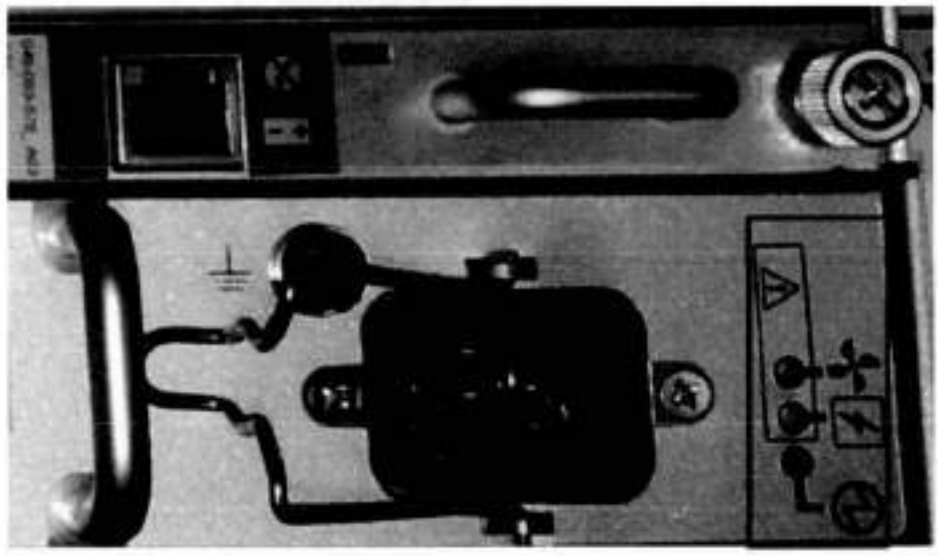


Figure 178. Power Supply A LEDs

Each shelf controller has two SAS ports. The port labeled with a circle symbol is the Host port, and the port labeled with a diamond symbol is the Expansion port. The Expansion ports are located on the outside, and the Host ports on the inside (reversed controller positions).

Table 225. Status lights visible from rear of disk enclosure

Light	Quantity	Color	Meaning
Controller Power	1 per Controller	Blue or Green	On when the Controller is powered on.
Controller Fault	1 per Controller	Amber	On when either the Controller or a SAS connection is faulty. On during power-on self-test
Host Link Active	1 per Controller	Blue	On when the host connection is active.
Expansion Link Active	1 per Controller	Blue	On when the expansion connection is active.
Power Supply Active	1 per power supply	Green	On when the power supply is operating.
Power Supply Fault*	1 per power supply	Amber	On when the power supply is faulty or is not receiving AC line voltage. Flashing when either a multiple blower or ambient over temperature condition has shut off DC power to the system.
Blower Fault*	1 per power supply	Amber	On when one of the blowers in the power supply is faulty.

*The ES30 and continue to run with a single power supply and three of its four blowers. Removing a power/cooling module constitutes a multiple blower fault condition, and powers down the shelf unless you replace a module within two minutes.

Ports

Depending on the model, a system has one to four dual- or quad-port SAS HBA cards or SAS I/O modules installed. The ES30 shelf has two controllers (B located above A). Each controller has two ports, a host and an expansion port.

17

ES40

This chapter contains the following topics:

Topics:

- ES40 overview
- Dimensions and weights
- Power requirements
- DAE-to-DAE copper cabling
- Product service tag

ES40 overview

Storage capacity can be increased by adding ES40 expansion shelves to DD6900, DD9400, and DD9900 systems.

The expansion shelves are organized by sets (or chains). The following table shows the number of ES40 shelves that can be in a set.

Table 226. ES40 shelves in a set

System	ES40 shelves
DD6900	1–7
DD9400	1–7
DD9900	1–7

For redundancy, a shelf set is connected to two separate SAS I/O modules or HBA cards on the controller, and all shelves within a set are connected to each other using dual paths.

Dimensions and weights

Table 227. Dimensions and weight

Dimensions	Vertical size	Weight (see note)
Height: 5.25 in (13.34 cm)	3 NEMA units	68 lb (30.8 kg) with 15 disks
Width: 17.62 in (44.75 cm)		
Depth: 14.0 in (35.6 cm)		
Note: The weight does not include mounting rails. Allow 5-10 lb (2.3-4.5 kg) for a rail set. The weights listed in this table do not describe enclosures with solid state disk drives with Flash memory (called Flash or SSD drives). These Flash drive modules weigh 20.8 ounces (1.3 lb) each.		

Power requiremements

The input current, power (VA), and dissipation per enclosure listed in this document are based on measurements of fully configured enclosures under worst-case operating conditions. Use the operating maximum values to plan the configuration of your storage system. These values represent either:

- the values for a single power supply line cord, or

- the sum of the values shared by the line cords of the combined power supplies in the same enclosure, with the division between the line cords and supplies at the current sharing ratio (approximately 50% each).

A failure of one of the combined power supplies per enclosure results in the remaining power supply supporting the full load. You must use a rackmount cabinet or rack with appropriate power distribution, and have main branch AC distribution that can handle these values for each enclosure in the cabinet.

Table 228. AC power specifications

Requirement	Description
AC line voltage	100 to 240V AC ± 10%, single-phase, 47 to 63 Hz
AC line current (operating maximum)	2.9 A max at 100V AC
	1.6 A max at 200V AC
Power consumption (operating maximum)	287 VA (281 W) max at 100V AC
	313 VA (277 W) max at 200V AC
Power factor	0.9 min at full load at 100V AC
	0.9 min at full load at 200V AC
Heat dissipation (operating maximum)	1.01 x 10^6 J/hr (959 Btu/hr) max at 100V AC
	1.01 x 10^6 J/hr (945 Btu/hr) max at 200V AC
In-rush current	30 A max for ½ line cycle, per line cord at 240V AC
Startup surge current	25 A peak max per line cord, max at any line voltage
AC protection	10 A fuse on each power supply, both Line and Neutral
AC inlet type	IEC320-C14 appliance coupler, per power zone
Ride-through time	30 ms min
Current sharing	Droop Load Sharing

NOTE:

- Ratings assume a fully loaded DAE that includes 2 power supplies and 12 worst case disk drive slot numbers.
- All power figures shown represent max normal operating numbers with the chassis running in a normal 20°C to 25°C ambient temperature environment. The chassis power numbers given may increase when running in a higher ambient temperature environment.
- For specific product configuration power numbers, refer to the EMC Power Calculator located on the internet at https://powercalculator.emc.com. The Power Calculator will provide the chassis power delta when operating in different ambient temperature ranges and configurations. However, it will only support products with an input voltage range of 200-240V ac.

Table 229. DC power specifications

Requirement	Description
DC line voltage	-39 to -72V DC (nominal -48 or -60 V power systems)
DC line current (operating maximum)	7.92 A max at -39V DC
	6.43 A max at -48V DC
	4.39 A max at -72V DC
Power consumption (operating maximum)	309 W max at -39V DC
	309 W max at -48V DC
	316 W max at -72V DC
Heat dissipation (operating maximum)	1.11 x 10^6 J/hr (1054 Btu/hr) max at -39V DC
	1.11 x 10^6 J/hr (1054 Btu/hr) max at -48V DC

Table 229. DC power specifications (continued)

Requirement	Description
	1.14 x 10^6 J/hr (1078 Btu/hr) max at -72V DC
In-rush current	20 A peak per requirements in EN300 132-2 Sect 4.7 limit curve
DC protection	20 A fuse in each power supply
DC inlet type	Positronics PLB3W3M1000
Mating DC connector	Positronics PLB3W3F7100A1
	Positronics Inc.
	http://www.connectpositronic.com
Ride-through time	5 ms min. (test condition: Vin = -40V DC)
Current sharing	Droop Load Sharing

NOTE:

- Ratings assume a fully loaded DAE that includes 2 power supplies and 15 maximum disk slot numbers.
- All power figures shown represent max normal operating numbers with the chassis running in a normal 20°C to 25°C ambient temperature environment. The chassis power numbers given may increase when running in a higher ambient temperature environment.
- The EMC Power Calculator does not support DC chassis.

DAE-to-DAE copper cabling

The expansion port interface to and between DAEs is copper cabling. The 100 Ω cables are keyed at either end, and available in 1- 10-meter lengths.

- DAE-to-DAE cables are SFF 8088 mini-SAS to mini-SAS.
- Keys are defined in the T10-SAS 2.1 specification.

Product service tag

The serial number is seven alphanumeric characters and found on the service tag.

18

FS15

This chapter contains the following topics:

Topics:

- Overview of FS15 SSD drives
- Site requirements
- FS15 hardware specifications
- FS15 front panel
- Back panel
- Status LEDs

Overview of FS15 SSD drives

The FS15 is an external shelf consisting of a specific number of SSD drives, depending upon the system, and are used to cache meta-data.

The SSDs for the FS15 shelf are 800GB 3WPD devices, which have positive performance and longevity characteristics.

Table 230. Number of SSD drives and model compatibilty

Number of Drives	Model
2	DD6300 with HA
5	• DD6800 with HA • DD9300 with HA
8	• DD9300 with HA • DD9500 - with or without HA
15	DD9500 - with or without HA

NOTE: Unused drive slots have drive fillers to improve airflow.

There are also upgrade kits available to add more SSDs if a system is expanded to have additional memory.

Upgrade Pack	Use
3 Drive Upgrade Pack	To create a 5 drive shelf from originally a 2 drive shelf or an 8 drive shelf from originally a 5 drive shelf
7 Drive Upgrade Pack	To create a 15 drive shelf from an 8 drive shelf

Site requirements

This table lists the FS15 site requirements.

Table 231. FS15 site requirements

Requirement	FS15 shelf
Vertical Space in Standard 19", 4-post Rack	3U. Do not use a two-post rack. See the slide rail and installation documentation in the packaging for installing in a rack.
Air Conditioning	Air conditioning that can cope with the maximum BTU/hr thermal rating.

Table 231. FS15 site requirements (continued)

Requirement	FS15 shelf
Temperature Controls	Adequate temperature control with a gradient (change) not to exceed 30° C in an hour.
Front Bezel Clearance	1.56 inches (4.0 cm) of unobstructed clearance.
Back Panel Clearance	5 inches (12.7 cm) of unobstructed clearance.
Airflow	In a closed or multi-unit rack, ensure that the unit has adequate airflow. If the equipment is mounted in an enclosed (as opposed to a four-post open rack), the front and rear doors should have 65% minimum open area for airflow. Whether in an open or enclosed rack, use filler panels to prevent hot air recirculation. The rack design and installation should take into consideration the maximum ambient operating temperature of the equipment, which is 35° C.
Power/ Grounding	Two single-phase AC power outlets with an earth ground conductor (safety ground). A safe electrical earth connection must be provided to each power cord. Voltage should be 100-120 VAC or 200-240 VAC; 50 or 60 Hz. Use only with branch circuits protected by a minimum 15A overcurrent protector. Plug the two power cords into separate branch circuit supplies for redundancy.

FS15 hardware specifications

NOTE: All ratings assume a fully configured FS15.

Table 232. FS15 hardware specifications

Specification	Description
AC line voltage	100 to 240 Vac ± 10%, single-phase, 47 to 63 Hz
AC line current (operating maximum)	2.8 A max at 100 Vac, 1.4 A max at 200 Vac
Power consumption (operating maximum)	280 VA (235 W) max
Power factor	0.98 min at full load, low voltage
Heat dissipation (operating maximum)	8.46 x 10^5 J/hr, (800 Btu/hr) max
Dimensions (rack mounted, with bezel)	• Width: 17.62" (45 cm) Depth: 14" (35.56cm) • Height: 5.25" (13.34cm) 3 RU
Maximum Weight	68 lbs (30.8 kg)
Operating Temperature	• Ambient temperature: 10° C to 35° C (50° F to 95° F) • Temperature gradient: 10° C/hr (180° F/hr) • Relative humidity extremes: 20% to 80% noncondensing
Recommended Operating Relative Humidity	40% to 55% noncondensing
Non-Operating Temperature	• Ambient temperature: -40° C to 65° C (-40° F to 149° F) • Temperature gradient: 25° C/hr (45°F/hr) • Relative humidity: 10% to 90% noncondensing

FS15 front panel

After you unlock and remove the snap-on bezel on the front panel, the 15 disks are visible. Disk numbers, as reported by system commands, range from 1 to 15. When facing the front panel, Disk 1 is located in the leftmost slot in the enclosure and Disk 15 in the rightmost slot.

Figure 179. FS15 front panel (bezel removed)

NOTE: The flanges or sheet metal on the FS15 show 0 to 14 but the software will refer to the logical numbering of 1 to 15.

Each disk in the enclosure has two LEDs. The disk's active LED glows green when the disk is functional. The disk fault LED glows amber when the disk has failed.

If there is a problem with the enclosure, the enclosure fault light is amber. The disk enclosure power light should be on (blue) when the shelf is powered on.

When replacing FS15 disks, a good practice is to run this command:

`disk beacon <enclosure-id>.<disk-id>`

NOTE: The `disk beacon` command causes the LED that signals normal operation to flash on the target disk. Enter `Ctrl-C` to stop the flash. You can also use the `enclosure beacon` command to check the LED to blink on every disk.

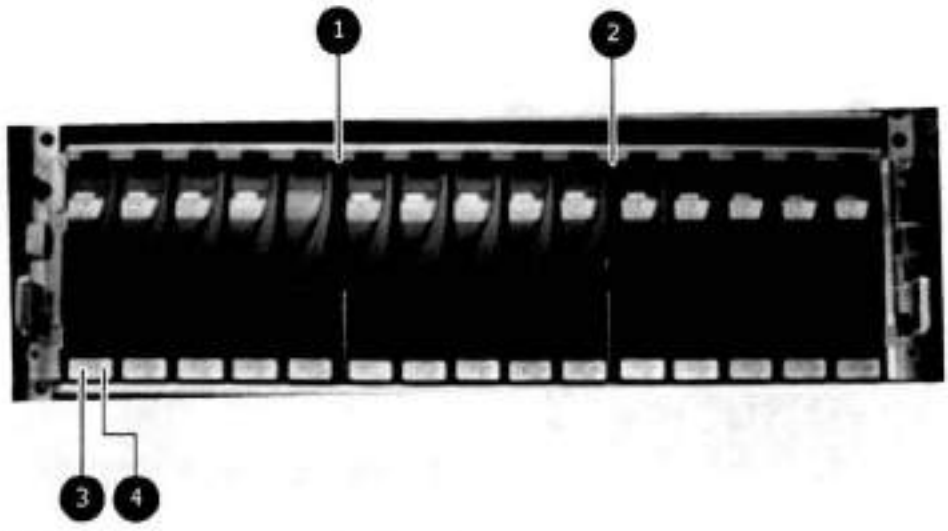


Figure 180. Front panel LEDs

1. Disk enclosure fault light
2. Disk enclosure power light
3. Disk active light
4. Disk fault light

Table 233. Status lights visible from front of disk enclosure

Light	Quantity	Color	Meaning
Disk enclosure fault light	1	Amber	On when any fault condition exists; if the fault is not obvious from a disk module light, look at the back of the disk enclosure.
Disk enclosure power light	1	Blue	Power to enclosure is on.
Disk active light	1 per disk module	Green	No LED when the slot is empty or has a filler module. Also, off when the disk is powered down by command; for example, the result of a temperature fault.

Table 233. Status lights visible from front of disk enclosure (continued)

Light	Quantity	Color	Meaning
			Fast blinking when the SATA/SAS drive is powered up but not spinning; this is a normal part of the spin-up sequence, occurring during the spin-up delays of a slot. On when the drive has power but is not handing any I/O activity (the ready state. Slow blinking when the drive is spinning and handling I/O activity.
Disk fault light	1 per disk module	Amber	On when the disk module is faulty, or as an indication to replace the drive.

Back panel

For redundancy, the shelf has two identical power supply/cooling modules and two identical shelf controllers which are placed in reverse order.

NOTE: When replacing a component, note its orientation before removing it. Insert the replacement in the same position.

Power supply A and controller A are located at the bottom of the chassis, and power supply B and controller B are located at the top of the chassis.

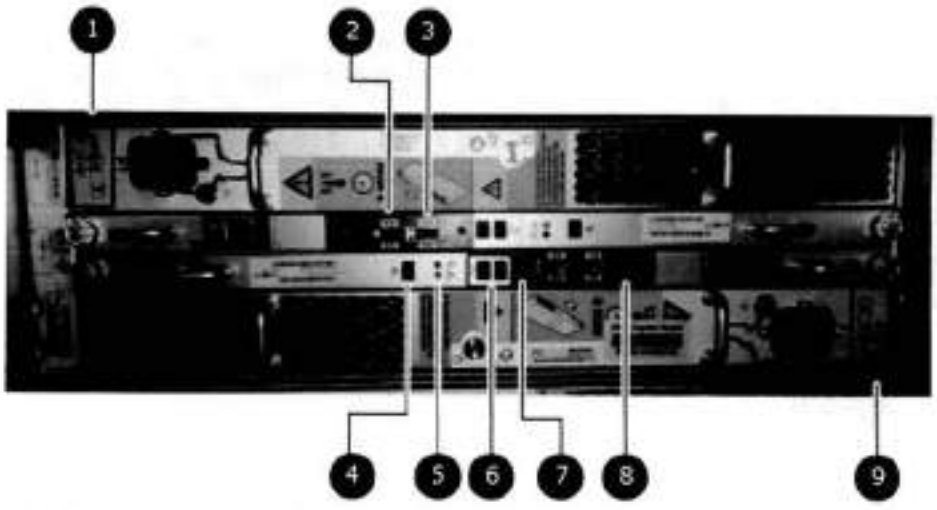


Figure 181. Back panel: Power modules and controllers

1. LEDs
   - Power supply B: Power LED
   - Power fault: Amber
   - Blower fault: Amber
2. Expansion (Out)
3. Host (In)
4. Enclosure address (not used)
5. Power (Green) or Fault (Amber)
6. Bus ID (not used)
7. Host link active
8. Expansion link active
9. LEDs
   - Power supply A Power LED
   - Power fault: Amber
   - Blower fault: Amber

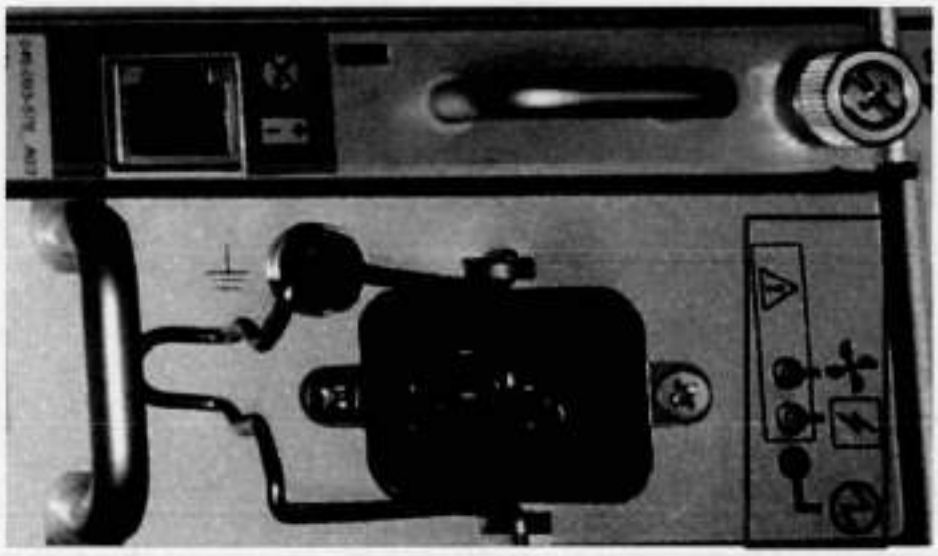


Figure 182. Power Supply A LEDs

Each shelf controller has two SAS ports. The port labeled with a circle symbol is the Host port, and the port labeled with a diamond symbol is the Expansion port. The Expansion ports are located on the outside, and the Host ports on the inside (reversed controller positions).

Table 234. Status lights visible from rear of disk enclosure

Light	Quantity	Color	Meaning
Controller Power	1 per Controller	Blue or Green	On when the Controller is powered on.
Controller Fault	1 per Controller	Amber	On when either the Controller or a SAS connection is faulty. On during power-on self-test
Host Link Active	1 per Controller	Blue	On when the host connection is active.
Expansion Link Active	1 per Controller	Blue	On when the expansion connection is active.
Power Supply Active	1 per power supply	Green	On when the power supply is operating.
Power Supply Fault*	1 per power supply	Amber	On when the power supply is faulty or is not receiving AC line voltage. Flashing when either a multiple blower or ambient over temperature condition has shut off DC power to the system.
Blower Fault*	1 per power supply	Amber	On when one of the blowers in the power supply is faulty.

*The ES30 and continue to run with a single power supply and three of its four blowers. Removing a power/cooling module constitutes a multiple blower fault condition, and powers down the shelf unless you replace a module within two minutes.

Status LEDs

Verify the status by checking the LEDs. Controller B is located above Controller A in the center of the rear panel. The power supply/cooling units are above and below the controllers.

Facing the back panel of the FS15, the Expander ports are the outer of the two ports; the Host ports are the inner of the two ports. The ports are identified by symbols on the rear panel: a circle symbol indicates a Host port; a diamond symbol indicates an Expander port.

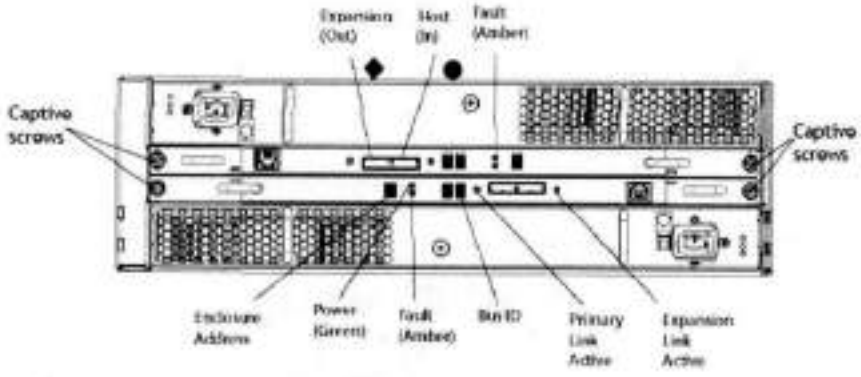


Figure 183. Rear panel overview

Table 235. Status LEDs

Light	Quantity	Color	Meaning
Controller power	1 per controller	Green	On when the controller is powered on
Controller failure	1 per controller	Amber	On when either the controller or a SAS connection has failed. On during a power-on self test.
Host link active	1 per controller	Blue	On when the host connection is active
Expansion link active	1 per controller	Blue	On when the expansion host is active

19

FS25

This chapter contains the following topics:

Topics:

- Overview of FS25 SSD drives
- Dimensions and weight
- Power requirements
- DAE-to-DAE copper cabling
- Product service tag

Overview of FS25 SSD drives

The FS25 is an external shelf consisting of a specific number of SSD drives, depending upon the system, and are used to cache meta-data.

Table 236. Number of SSD drives and model compatibilty

Number of Drives	Model
2	DD6900 only with HA
5	DD9400 only with HA
10	DD9900

NOTE: Unused drive slots have drive fillers to improve airflow.

Dimensions and weight

Table 237. Dimensions and weight

Dimensions	Vertical size	Weight (see note)
Height: 3.40 in (8.64 cm)	2 NEMA units	44.61 lb (20.23 kg) with 25 disks
Width: 17.50 in (44.45 cm)		
Depth: 14.0 in (35.56 cm)		
Note: The weight does not include mounting rails. Allow 5-10 lb (2.3-4.5 kg) for a rail set. The weights listed in this table do not describe enclosures with solid state disk drives with Flash memory (called Flash or SSD drives). These Flash drive modules weigh 20.8 ounces (1.3 lb) each.		

Power requirements

The input current, power (VA), and heat dissipation per enclosure listed in this document are based on measurements of fully configured enclosures under worst-case operating conditions. Use the operating maximum values to plan the configuration of your storage system. These values represent either:

- values for a single power supply line cord, or
- the sum of the values shared by the line cords of the combined power supplies in the same enclosure, with the division between the line cords and supplies at the current sharing ratio (approximately 50% each).

A failure of one of the combined power supplies per enclosure results in the remaining power supply supporting the full load. You must use a rackmount cabinet or rack with appropriate power distribution, and have main branch AC distribution that can handle these values for each enclosure in the cabinet.

Table 238. AC power specifications

Requirement	Description
AC line voltage	100 to 240V AC ± 10%, single-phase, 47 to 63 Hz
AC line current (operating maximum)	4.5 A max at 100V AC
	2.4 A max at 200V AC
Power consumption (operating maximum)	453 VA (432 W) max, at 100V AC
	585 VA (427 W) max, at 200V AC
Power factor	0.95 min at full load, @ 100V AC
	0.95 min at full load, @ 200Vac
Heat dissipation (normal operating maximum)	1.56 x 10^6 J/hr, (1,474 Btu/hr.) max @ 100V AC
	1.54 x 10^6 J/hr, (1,457 Btu/hr) max @ 200Vac
In-rush current	30 Apk "cold" per line cord at any line voltage
Startup surge current	40 Apk "hot" per line cord, at any line voltage
AC protection	15 A fuse on each power supply, single line
AC inlet type	IEC320-C14 appliance coupler, per power zone
Ride-through time	12 ms min
Current sharing	± 5% of full load, between power supplies

NOTE:

- Ratings assume a fully loaded DAE that includes 2 power supplies and 25 worst case disk drive slot numbers.
- All power figures shown represent max normal operating numbers with the chassis running in a normal 20°C to 25°C ambient temperature environment. The chassis power numbers given may increase when running in a higher ambient temperature environment.
- For specific product configuration power numbers, refer to the EMC Power Calculator located on the internet at https://powercalculator.emc.com. The Power Calculator will provide the chassis power delta when operating in different ambient temperature ranges and configurations. However, it will only support products with an input voltage range of 200-240V ac.

Table 239. DC power specifications

Requirement	Description
DC line voltage	-39 to -72V DC (nominal -48 or -60 V power systems)
DC line current (operating maximum)	11.0 A max at -39V DC
	9.10 A max at -48V DC
	6.20 A max at -72V DC
Power consumption (operating maximum)	428 W max at -39V DC
	437 W max at -48V DC
	448 W max at -72V DC
Heat dissipation (operating maximum)	1.54 x 10^6 J/hr (1460 Btu/hr) max at -39V DC
	1.57 x 10^3 J/hr (1491 Btu/hr) max at -48V DC
	1.61 x 10^6 J/hr (1529 Btu/hr) max at -72V DC
In-rush current	40 A peak per requirements in EN300 132-2 Sect 4.7 limit curve

Table 239. DC power specifications (continued)

Requirement	Description
DC protection	50 A fuse in each power supply
DC inlet type	Positronics PLBH3W3M4B0A1/AA
Mating DC connector	Positronics PLBH3W3F0000/AA
	Positronics Inc.
	http://www.connectpositronic.com
Ride-through time	1 ms min. at -50V input
Current sharing	±5% of full load, between power supplies

NOTE:

- Ratings assume a fully loaded DAE that includes 2 power supplies and 25 maximum disk slot numbers.
- All power figures shown represent max normal operating numbers with the chassis running in a normal 20°C to 25°C ambient temperature environment. The chassis power numbers given may increase when running in a higher ambient temperature environment.
- The EMC Power Calculator does not support DC chassis.

DAE-to-DAE copper cabling

The expansion port interface to and between DAEs is copper cabling. The 100 Ω cables are keyed at either end, and available in 1- 10-meter lengths.

- DAE-to-DAE cables are SFF 8088 mini-SAS to mini-SAS.
- Keys are defined in the T10–SAS 2.1 specification.

Product service tag

The serial number is seven alphanumeric characters and found on the service tag.

Index

S

Dell EMC PowerProtect DD Management Center (DDMC)

Guia de instalação e administração

7.7

Setembro de 2021
Rev. 01

DELL EMC

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam você a usar melhor o seu produto.

CUIDADO: **um AVISO indica possíveis danos ao hardware ou a possibilidade de perda de dados e informa como evitar o problema.**

ATENÇÃO: uma ADVERTÊNCIA indica possíveis danos à propriedade, lesões corporais ou risco de morte.

Índice

Histórico de revisões

A seguinte tabela apresenta o histórico de revisões deste documento.

Tabela 1. Histórico de revisão do documento

Revisão	Data	Descrição
01	Setembro 2021	Publicação inicial

1

Visão geral do DDMC no PowerProtect

Tópicos:

- Introdução ao PowerProtect DDMC
- Recursos e limitações do DDMC
- Diferenças entre o DDMC e o PowerProtect DD System Manager

Introdução ao PowerProtect DDMC

O DDMC é uma solução escalável e baseada em sistema virtual para o gerenciamento centralizado de diversos sistemas DD e sistemas virtuais de proteção de dados (instâncias do PowerProtect DDVE).

O DDMC é composto de páginas baseadas em navegador e é instalado e executado em uma plataforma VMware. Ele:

- fornece dados históricos e atuais de todos os sistemas gerenciados, com a apresentação de assuntos que variam de resumos de todo o site a detalhes granulares para um objeto selecionado.
- projeta a capacidade e disponibilidade do sistema, a integridade do limite de capacidade e o fator de compactação
- monitora o armazenamento em diversos sistemas com a opção Secure Multitenancy, backup do DD Boost e replicação.

NOTA: A opção Secure Multitenancy é compatível apenas com o DDVE 3.0 e posterior.

Recursos e limitações do DDMC

Os recursos avançados do DDMC ajudam a gerenciar todos os sistemas DD por meio de uma interface de usuário conveniente.

Esses recursos permitem que você:

- Monitore e gerencie
  - Monitore a integridade e a operação dos objetos gerenciados em um painel configurável pelo usuário
  - Exiba a capacidade de armazenamento de todo o site, mostrando os totais de uso agregado, inclusive o Cloud Tier
  - Represente em gráfico os dados atuais e históricos sobre o uso de espaço, consumo de dados e as tendências de dados gravados diariamente
  - Gerencie o recurso Secure MultiTenancy (SMT), especialmente para configurar e monitorar o acesso ao DD Boost
  - Monitore o status operacional de replicações configuradas e defina limites que gerem alertas (enviados para o registro de alertas) quando as replicações atrasarem
  - Gerencie o acesso do usuário por meio de definições configuráveis do RBAC (Role-Based Access Control, controle de acesso baseado em função)
- Gere estimativas e relatórios
  - Estime as necessidades de capacidade projetada com base em tendências históricas e identifique datas específicas (do passado e do futuro) para fins de comparação de uso
  - Gere relatórios de uso e desempenho sob demanda ou defina uma lista de e-mail e agendamento para facilitar o gerenciamento proativo
  - Processe alertas de todos os sistemas DD gerenciados, inclusive Cloud Tier, e visualize-os em uma única lista
  - A integração do gateway (GW) do Secure Remote Service (ESRS) V3 proporciona transferência segura de mensagens ao suporte da Dell
- Atue simultaneamente em vários sistemas DD
  - Recursos de gerenciamento de vários sistemas com o DDMC e recursos completos de gerenciamento de um sistema único com o DD System Manager
  - Crie agrupamentos personalizados dos sistemas Data Domain ou PowerProtect gerenciados, organizados de modo eficiente e intencional
  - Aplique grupos e propriedades a objetos gerenciados para personalizar como o conteúdo é exibido e a melhor forma de representar a infraestrutura

- Configure os grupos de usuários do Secure MultiTenancy e as unidades de grupos de usuários para os sistemas DD gerenciados individualmente, ou em grupos, como acesso do usuário e atualizações do DDOS

Recursos e protocolos não compatíveis

Os protocolos e recursos a seguir não são compatíveis com o DDMC e devem ser considerados como limitações do produto:

- Nenhum backup no DDMC
- Nenhum file system
- DD Boost
- Software Replicator
- DD Encryption
- NFS
- Autenticação Kerberos

Os comandos do DDOS relacionados a esses recursos não compatíveis não possuem suporte no DDMC.

Diferenças entre o DDMC e o PowerProtect DD System Manager

O DDMC difere do DD System Manager das seguintes maneiras:

- O DDMC pode gerenciar até 150 sistemas PowerProtect DD, enquanto o DD System Manager é uma ferramenta para gerenciamento de sistema único.

  NOTA: O DDMC não pode gerenciar os sistemas PowerProtect DP Series (DPA).

  - O DDMC inclui a capacidade de gerenciar sistemas com alta disponibilidade (HA), nível da nuvem e instâncias do DDVE.
- O DDMC pode realizar uma atualização em grupos de sistemas simultaneamente.
- O DDMC agrega dados de desempenho e armazenamento e compara informações operacionais para todos os sistemas gerenciados. O DD System Manager não agrega dados de armazenamento ou dados de desempenho de vários sistemas nem pode comparar informações operacionais em sistemas.
- O DDMC não gerencia diretamente o armazenamento. O DD System Manager gerencia diretamente o armazenamento (usando VTL, CIFS, NFS, DD Boost e assim por diante).
- O DDMC não pode configurar e gerenciar nenhuma replicação ou criptografia.

2

Planejar o ambiente do DDMC

Tópicos:

- Requisitos do sistema
- Determinando os requisitos da VMware
- Back up e restauração

Requisitos do sistema

Os requisitos de hardware de máquina virtual são informados nesta tabela.

Tabela 2. Requisitos do sistema

Número de sistemas gerenciados	CPU virtual (vCPU)	memória (GB)	Tamanho do disco da VM - instalação básica + banco de dados + disco de serviços DD (GB)
1 a 150	4 vCPUs	8	40 + 200 + 100

NOTA: Essas configurações são fixas para todas as combinações e a alteração de qualquer um dos componentes individuais dessas configurações não é suportada. Não é possível aumentar a memória, alterar as configurações da CPU e assim por diante.

Determinando os requisitos da VMware

Os requisitos da VMware incluem:

- Requisitos do sistema de hardware e software VMware na página 10
- Aplicativos de software adicionais da VMware na página 11

Requisitos do sistema de hardware e software VMware

O hardware e o software VMware requeridos para hospedar uma instalação do DDMC podem ser:

- A instalação do vCenter Server, que acomoda diversas máquinas virtuais, sendo uma delas o DDMC. O servidor é onde as máquinas virtuais são configuradas, provisionadas e gerenciadas.
- Um dos seguintes:
  - ESXi 6.5
  - ESXi 6.7
  - ESXi 7.0
- vSphere Client, uma interface de usuário que permite aos usuários se conectarem remotamente a qualquer um dos tipos de servidor para realizar o gerenciamento remoto.

O armazenamento para a instalação dos produtos VMware pode ser fornecido usando:

- NAS (discos virtuais em NFS)
- SAN (discos virtuais em VMFS)

Requisitos de alta disponibilidade (HA)

Se uma configuração de alta disponibilidade for necessária, use a opção de software VMware de sua escolha para implementar essa configuração.

Aplicativos de software adicionais da VMware

O DDMC é um vApp de VMware. Para aumentar a confiabilidade da instalação do DDMC, os aplicativos a seguir são úteis.

VMware vSphere High Availability (HA)

O VMware vSphere High Availability (HA) oferece alta disponibilidade econômica para qualquer aplicativo em execução em uma máquina virtual, independentemente de seu sistema operacional ou configuração de hardware subjacente.

VMware vSphere Fault Tolerance (FT)

O VMware vSphere Fault Tolerance (FT) oferece tempo de inatividade nulo, perda de dados nula e disponibilidade contínua para aplicativos, sem o custo e a complexidade de soluções de clustering de software ou hardware tradicionais.

Back up e restauração

Qualquer processo que cria e restaura um snapshot de toda a máquina virtual pode proteger com sucesso a instalação do DDMC.

É altamente recomendável que você execute um snapshot antes de realizar um procedimento de upgrade.

O DDMC não depende de ter qualquer integração ao software para backup.

Depois que o snapshot é restaurado, o DDMC executa automaticamente qualquer recuperação de aplicativos necessária.

As opções de software para backup adequadas incluem o VMware Data Recovery (VDR), o Avamar, e assim por diante.

Como ocorre com qualquer software de proteção de dados, certifique-se de testar sua configuração depois de instalar o software para backup escolhido.

NOTA: O uso de clonagem não foi validado.

3

Como começar

Tópicos:

- Pré-requisitos
- Baixando o DDMC
- Instalando o DDMC em um ambiente VMware
- Hyper-V
- DDMC em uma máquina virtual baseada em kernel
- Implementando o DDMC na AWS (Amazon Web Services) usando o modelo Cloud Formation
- DDMC no Azure Marketplace
- Como implementar o DDMC na Google Cloud Platform (GCP)
- Implementar sistemas DDVE
- Ligar o DDMC
- Fazendo log-in e log-out no DDMC
- Adicionar (registrar) sistemas ao DDMC
- Continuar a configuração do DDMC
- Noções básicas sobre o RBAC no DDMC
- Visualizando os elementos de página do DDMC
- Acessando uma página do DDMC
- Organizando o painel de controle
- Organizando sistemas gerenciados
- Datacenter
- Exibindo informações de propriedade
- Gerenciando políticas de limite de intervalo de replicação
- Trabalhando com filtros

Pré-requisitos

Leia o capítulo Planejar o ambiente do DDMC na página 10 e verifique se os componentes necessários de hardware e software da VMware estão implementados no local. O guia também inclui descrições de produtos de software opcionais da VMware para backup e confiabilidade que garantem a operação ideal da instalação do DDMC.

Verifique o seguinte:

- Servidores e software do VMware vCenter ou VMware ESXi
- O aplicativo cliente VMware vSphere (o aplicativo cliente VMware vSphere só será necessário se estiver instalando no vSphere/vCenter. Ele não é necessário para o AWS, Azure, GCP, Hyper-V ou KVM.)
- CPU, memória, espaço em disco e recursos de rede suficientes
- Se instalar em um ou ambiente de nuvem ou Hyper-V e não puder usar credenciais baseadas em função, tenha informações disponíveis para criar um perfil de acesso.

Baixando o DDMC

O arquivo zip DDMC que você usa depende do ambiente no local no qual você está operando.

Etapas

1. Faça log-in no site de suporte usando suas credenciais (se já as tiver) ou registre-se para obter suas credenciais.
2. Selecione **Support by product** abaixo da caixa de pesquisa.
3. Use a caixa de pesquisa **Find a Product** para localizar o **DDMC**.

4. Na lista de categorias na caixa de pesquisa, selecione **Downloads**.
5. Selecione o link para baixar a versão apropriada do software.
6. Faça download do arquivo zip apropriado do DDMC para seu ambiente no local.

NOTA: DDMC no AWS, Azure e GCP estão disponíveis no marketplace de cada uma dessas nuvens públicas. A Dell EMC não fornece mais o arquivo de imagem para download.

Próximas etapas

Agora você pode instalar o software do DDMC na plataforma VMware.

Instalando o DDMC em um ambiente VMware

Há dois procedimentos para a instalação do arquivo `.ovf` e para a definição das configurações do DDMC.

- Instalando em um VMware vCenter Server na página 14
- Instalando em um servidor VMware ESXi na página 15

Veja a seguir um resumo das configurações padrão de fábrica e das configurações que podem ser definidas durante o procedimento de configuração.

Tabela 3. Instalação e definições de configuração

Configuração	Valores padrão
Nome	Nome para a máquina virtual do DDMC (o padrão é DDMC)
Nome de host	Nome de host completo
Endereço IP do gateway	Endereço IP do servidor do gateway
Número de série	Gerado automaticamente
Política de alocação de IP	Endereço IP DHCP ou fixo. Se o endereço IP for fixo, informe o endereço IP, a máscara de rede e as informações do gateway.
Servidores DNS	Nomes dos servidores DNS primário e secundário (obrigatório). Se for usado apenas um servidor primário no site, digite o nome do servidor primário no campo do servidor secundário também.
Servidor de e-mail	Endereço do servidor de e-mail para o site
Admin Email	Endereço de e-mail do administrador para o site
ASUP to Support	Ativado (padrão) ou desativado
Alerts to Support	Ativado (padrão) ou desativado
ASUP to Admin	Ativado ou desativado (padrão)
Alerts to Admin	Ativado ou desativado (padrão)
AM Email to Admin	Ativado ou desativado (padrão)
Network Ports	eth0a – habilitada para DHCP; eth0b – desabilitada
SSH, HTTPS	Habilitado por padrão
ASUP and Alerts	autosupport@autosupport.datadomain.com
AM Email	É executado diariamente às 8h
ASUP	É executado diariamente às 6h
sysadmin password	O padrão é "changeme". Após o log-in inicial, a senha deverá ser alterada para algo que atenda aos requisitos de segurança do site. Faça isso antes de começar a adicionar sistemas Data Domain ou PowerProtect.

Instalando em um VMware vCenter Server

Pré-requisitos

1. Faça download do software DDMC, conforme descrito em como fazer download do DDMC.
2. Abra o vSphere client, digite o seguinte e selecione **Login**:
   - O endereço IP ou o nome do host do VMware vCenter Server em que o DDMC será instalado
   - ID e senha de administrador para o VMware Server

Sobre esta tarefa

NOTA: A tabela a seguir corresponde ao Assistente da VMware.

Tabela 4. Instalar o DDMC em um VMware vCenter Server

Etapa do assistente de implementação	Descrição
Inicie o Assistente de implementação da máquina virtual	Use o Assistente de implementação da VMware para implementar a instância do DDMC.
Detalhes do modelo OVF	Implemente a partir do arquivo `.ovf` ou descompacte a pasta vCenter para obter os arquivos `.ovf` e `vmdk`.
Nome e local	Opcionalmente, digite um nome (o padrão é "DDMC") e selecione um local de instalação. Esse nome identifica a máquina virtual no servidor VMware. Ele não se torna um hostname na LAN.
Configuração de implementação	A configuração padrão não pode ser alterada.
Host/Cluster	Selecione um host ou cluster para a instalação do DDMC.
Datastore	Selecione o datastore onde os dados serão armazenados. Para obter o melhor desempenho, o Data Domain recomenda que você use um datastore dedicado.
Disk Format	Selecione o tipo de formato do disco. **Thin Provisioned** o formato do disco aloca dinamicamente a capacidade de armazenamento. **Thick Provisioned** o formato do disco aloca todo o armazenamento agora (recomendado).
IP Address Allocation	Selecione a configuração do endereço IP. **Fixed** ou **DHCP**. O DDMC não dá suporte a **Transient**. Uma configuração de endereço **Fixed** também inclui a máscara de rede, o endereço IP do gateway e o endereço do servidor DNS primário e secundário.
Propriedades	Forneça os seguintes detalhes do sistema: • Identificação do sistema – **Host name**: requer um hostname do DDMC totalmente qualificado • Informações de rede – **IP Address**: endereço IP do DDMC • Informações de rede – **Network Mask**: máscara de rede do DDMC • Informações de rede – **Gateway IP Address**: endereço IP do gateway do DDMC • Informações de rede – **Primary DNS Server**: endereço IP do servidor de nome principal do DDMC • Informações de rede – **Secondary DNS Server**: endereço IP do servidor de nome secundário do DDMC • Notificação por e-mail – **Mail Server**: requer um hostname para o servidor de e-mail que o DDMC usará para enviar e-mails • Notificação por e-mail – **Alerts**: enviar notificações de alerta • Notificação por e-mail – **Autosupport**: enviar informações do autosupport • Contato administrativo – **Administrator's Email**: requer um endereço de e-mail para um administrador do DDMC • Contato administrativo – **Alerts**: envia notificações de alerta para o endereço de e-mail do administrador • Contato administrativo – **Daily Alert Summary**: envia o resumo de alerta diário para o endereço de e-mail do administrador

Tabela 4. Instalar o DDMC em um VMware vCenter Server (continuação)

Etapa do assistente de implementação	Descrição
	• Contato administrativo - **Autosupport**: envia informações de autosupport para o endereço de e-mail do administrador
Está tudo pronto para a conclusão	Analise o resumo de configuração e encerre o assistente.

Essa configuração inicial não pode ser executada novamente para alterar as configurações. Após concluir a configuração inicial, você deverá usar a interface de linha de comando do DDMC para todas as configurações que desejar alterar.

Instalando em um servidor VMware ESXi

Pré-requisitos

1. Faça download do software DDMC, conforme descrito em como fazer download do DDMC.
2. Abra o vSphere client, digite o seguinte e selecione **Login**:
   - O endereço IP ou o nome do host do VMware ESXi Server em que o DDMC será instalado
   - ID e senha de administrador para o VMware Server

Sobre esta tarefa

NOTA: A tabela a seguir corresponde ao Assistente da VMware.

Tabela 5. Como instalar o DDMC em um VMware ESXi Server

Etapa de instalação	Descrição
Inicie o Assistente de implementação da máquina virtual	Use o Assistente de implementação da VMware para implementar a instância do DDMC.
Detalhes do modelo OVF	Implemente a partir do arquivo `.ovf` ou descompacte a pasta ESXi para obter os arquivos `.ovf` e `vmdk`.
Nome e local	Opcionalmente, digite um nome (o padrão é "DDMC <número da versão>") e selecione um local de instalação. Esse nome identifica a máquina virtual no servidor VMware. Ele não se torna um hostname na LAN.
Configuração de implementação	A configuração padrão não pode ser alterada.
Datastore	Selecione o datastore onde os dados serão armazenados. Para obter o melhor desempenho, a Dell EMC recomenda que você use um datastore dedicado.
Disk Format	Selecione o tipo de formato do disco. **Thin Provisioned** o formato do disco aloca dinamicamente a capacidade de armazenamento. **Thick Provisioned** o formato do disco aloca todo o armazenamento agora (recomendado).
Está tudo pronto para a conclusão	Analise o resumo de configuração e encerre o assistente.

Essa configuração inicial não pode ser executada novamente para alterar as configurações. Após concluir a configuração inicial, você deverá usar a interface de linha de comando do DDMC para todas as configurações que desejar alterar.

Hyper-V

Essa versão do DDMC permite criar máquinas virtuais usando o Microsoft Hyper-V para Windows.

Requisitos de implementação do Hyper-V

O DDMC em Hyper-V usa 4 CPUs, 8 GB de RAM e 350 GB de espaço em disco quando implementado.

Configurar o Hyper-V

Para configurar o Hyper-V, acesse o site do Microsoft Windows Server (2012 R2 ou 2016) e siga as instruções da página de instalação.

Baixe o pacote do Hyper-V para o DDMC.

Acesse o site de suporte e baixe o arquivo ZIP do Hyper-V de acordo com a versão do DDMC para o servidor do Hyper-V.

Implantar o pacote do Hyper-V para o DDMC

Sobre esta tarefa

O pacote Hyper-V contém:

- `ddmc-installer-sc.psl`: o script PowerShell usado para a implementação do DDMC no Microsoft System Center
- `README.txt`: Contém informações adicionais sobre as etapas necessárias para implementar o pacote.
- `ddmc-N.N.N.N-xxxxxx.vhd`: o disco de inicialização
- `ddmc-installer.psl`: o script do PowerShell necessário para a implantação do DDMC em um Microsoft Windows Server 2012 R2 ou Windows Server 2016 com Hyper-V Server.

Etapas

1. Descompacte o pacote `ddmc-N.N.N.N-xxxxxx-hyperv.zip` em uma pasta.
   O script deve ser baixado no Windows server (2012 R2 or 2016).
2. Abra o prompt do Power Shell como administrador.
3. Execute o seguinte script e especifique o nome da máquina virtual do DDMC quando solicitado: `.\ddmc-installer.psl`

DDMC em uma máquina virtual baseada em kernel

O DDMC implementado em uma KVM é compatível somente com processadores Intel. As seguintes distribuições do Linux são compatíveis:

Tabela 6. Distribuições compatíveis do Linux

Distribuição do Linux	Versão
RedHat	7.7, 7.6 e 7.8
SUSE	SLES 12-SP2
Ubuntu	14.04 e 16.04

Implementando o DDMC em uma máquina virtual baseada em kernel

Pré-requisitos

Etapas

1. Baixe e extraia o arquivo ZIP instalável da KVM. O nome do arquivo é `ddmc-kvm-<branch number>-<build number>.tar.gz`.
2. Copie o arquivo TAR para o sistema Linux em que a KVM está instalada e na partição em que as VMs estão armazenadas. Crie um diretório para a nova VM com o DDMC.
3. Descompacte o arquivo TAR. Ele criará um diretório.
   O diretório tem os seguintes arquivos:
   - `DDMC_README.txt`: arquivo de ajuda na implementação da VM na KVM.

- `kvm-ddmc-installer.sh`: DDMC deployment script, which automatically setups CPU, RAM, DISK, NVRAM configuration
- `ddmc-<branch number>-<build number>.qcow2`: Root disk for VM

```
root@ddve-ucs55d:/mnt/ucs55d-das1/ddmc_set/ddmc1# tar -xzvf ddmc-
kvm-0.6120.12.0-566688.tar.gz
ddmc-kvm-0.6120.12.0-566688/
ddmc-kvm-0.6120.12.0-566688/DDMC_README.txt
ddmc-kvm-0.6120.12.0-566688/kvm-ddmc-installer.sh
ddmc-kvm-0.6120.12.0-566688/ddmc-0.6120.12.0-566688.qcow2
```

4. Execute o script `kvm-ddmc-installer.sh` para implementar a VM do DDMC. Depois que a VM for implementada, ela será ativada.

```
root@ddve-ucs55d:/mnt/ucs55d-das1/ddmc_set/ddmc1/ddmc-kvm-0.6120.12.0-566688# ./kvm-ddmc-
installer.sh -n GS-DDMC -r /data/
Distribution:ubuntu Version:16.04
A verificação da versão do host foi concluída.
Basic validation done.
Convert the root disk to raw...
Disk convert done.
root disk:/data/GS-DDMC cpu:4 mem_value:8192 $ bridge:virbr0
Start creating DB disk, it may take 20-30 minutes...
DB disk file has been created successfully.
Start creating SERVICE disk, it may take 10-20 minutes...
SERVICE disk file has been created successfully.
Domain GS-DDMC defined from config.xml

Domain GS-DDMC marked as autostarted

Domain GS-DDMC started

DDMC instance has been created successfully!
Waiting to get ip address on the vm...
IP address not available yet. Retrying in 30 seconds...
IP address not available yet. Retrying in 30 seconds...
IP address not available yet. Retrying in 30 seconds...
IP address not available yet. Retrying in 30 seconds...
IP address of the vm is xxx.xxx.xxx.xxx
```

5. Faça log-in na GUI do host da KVM. Execute o comando `virt-manager`, e a GUI de gerenciamento de VMs da KVM será exibida.
6. Conecte-se ao console e verifique o endereço IP. Agora você pode configurar o DDMC remotamente.

Adicionar o Dell EMC PowerProtect DD Virtual Edition ao DDMC

Etapas

1. Implemente o PowerProtect DDVE na KVM. (Para obter mais informações, consulte o Guia de Administração e Instalação do DDVE.)
2. Veja os endereços IP do DDVE que serão adicionados ao DDMC para o gerenciamento.
3. Faça log-in no DDMC.
4. Execute o comando a seguir no DDMC para adicionar o DDVE do sistema DDVE gerenciado ao DDMC: `# managed-system add <IP address of DDVE> inbound-proxy <IP address of DDMC> outbound-proxy <IP address of DDVE>.`

```
managed-system add 10.98.99.237 inbound-proxy 10.98.99.225 outbound-proxy 10.98.99.237
The SHA1 fingerprint for the remote host's CA certificate
is46:3D:3C:B3:38:CE:31:E1:CE:1B:E6:4B:41:42:D3:78:00:D9:01:60
Do you want to trust this certificate?  Are you sure? (yes|no|  [no]: yes

** Once added, all "admin" role users on this DDMC
   will operate on "10.98.99.237" system with "admin" role.
And all "limited-admin" role users on this DDMC
   will operate on "10.98.99.237" system with "user" role if the system version is 5.7 and
below, or "limited-admin" role if the system version is 6.0 and above.

To allow "10.98.99.237" to be managed by this DDMC,
Enter "10.98.99.237" sysadmin password: ok, proceeding.
10.98.99.237 is added.
It may take a while to collect all information for "10.98.99.237".
sysadmin@ddmcset-ddmc-1# managed-system show
```

```
Host Name                          Serial Number    State     Status   DD OS Version
Sync Time              Type
-------------------------------    -------------    -------   ------   -----------------
----------------   ----------
ddmcset-ddve-1.datadomain.com      AUDVTPCKZ1SY5W   managed   online   6.6120.12.0-564400
Jun  6 2017 12:22   standalone
-------------------------------    -------------    -------   ------   -----------------
----------------   ----------
```

5. Em um navegador compatível, digite `http://<IP address of DDMC>` para conectar-se à GUI do DDMC.

Resultados

O sistema DD VE será adicionado em **Systems** > **Inventory**.

Implementando o DDMC na AWS (Amazon Web Services) usando o modelo Cloud Formation

Etapas

1. Acesse o AWS Marketplace: https://aws.amazon.com/marketplace
2. Pesquise **PowerProtect DD Management Center**.
3. Selecione **DellEMC PowerProtect DD Management Center (DDMC) <version number>**, e clique em **Continue to Subscribe**.
4. Clique em **Continue to Configuration**
5. Selecione as seguintes configurações e, em seguida, clique em **Continue to Launch**.
   - Opção de cumprimento: Método: Selecione **CloudFormation template**
   - Software Version: selecione a versão correta.
   - Region: selecione onde o DDMC deve ser implementado.
6. Analise os detalhes de configuração do DDMC, selecione o modelo **Launch the CloudFormation** e, em seguida, selecione **Launch**.
7. Clique em **Next**.
8. Informe os valores a seguir para criar a pilha:
   - Nome da pilha
   - DDMC Name Tag
   - Par de chaves - selecione um par de chaves existente na lista suspensa
   - ID da sub-rede
   - Grupos de segurança
9. Continue com a configuração da pilha, conforme necessário. Clique em **Next.**.
10. Analise a configuração da pilha e clique em **Create Stack**.
11. Verifique o status da pilha criada. Após a conclusão da criação da pilha, navegue até a página do EC2 e selecione a região na qual implementou o DDMC. Use a etiqueta de nome do DDMC da etapa 8 e verifique se a instância do EC2 correspondente está em execução.

DDMC no Azure Marketplace

Sobre esta tarefa

Execute as etapas a seguir para implementar o DDMC do Azure Marketplace.

Etapas

1. Faça log-in no portal do Azure. https://portal.azure.com
2. Pesquise por "Dell EMC" e encontre o **PowerProtect DD Management Center** no Azure Marketplace.
3. Selecione um plano e clique em **Create** para iniciar a implementação.
4. Preencha as informações de configurações na guia **Basics** e clique em **Next: Disks**.

Grupo de recursos	Especifique o grupo de recursos do DDMC.

Nome da máquina virtual	Digite o nome do DDMC.
Região	Região de implementação do DDMC
Imagem	Selecione a versão do DDMC.
Tamanho	Selecione **Standard_D4s_v3**
Nome de usuário	Digite **sysadmin**
Password	Senha para sysadmin
Regras da porta de entrada	Selecione **Allow selected ports**
Selecione as portas de entrada.	Selecione HTTP(80), HTTPS(443), and SSH(22)

5. Na guia **Disks** , configure o armazenamento em disco para o DDMC e, em seguida, clique em **Next: Networking**.
   - Tipo de disco do sistema operacional: selecione o tipo com base em sua necessidade
   - Host caching: selecione **None**
   - O disco de banco de dados e o disco de serviço foram configurados e adicionados automaticamente durante a implementação.
6. Na guia **Networking**, defina a conectividade de rede para este DDMC.

Rede virtual	Vnet para esse DDMC
sub-rede	especifique a sub-rede deste DDMC
IP público	A recomendação é implementar o DDMC em uma sub-rede privada e deixar o IP público como **None**.
Grupo de segurança de rede NIC	configuração de rede
Portas de entrada públicas	Permitir portas selecionadas
Selecionar portas de entrada	Selecione HTTP(80), HTTPS(443), SSH(22), RDP(3389)
Sistema de rede acelerado	Desligado
Balanceamento de carga	Não

7. Na guia **Management**, configure as opções de monitoramento e gerenciamento do DDMC.
   - Boot diagnostics: selecione On se você quiser capturar o resultado do console serial do DDMC para ajudar a diagnosticar um problema de inicialização
   - System assigned managed identity: selecione Off
   - Enable auto-shutdown: selecione Off
8. Na guia **Tags**, crie uma tag, por exemplo, Nome, <o nome deste DDMC>, para o DDMC do gerenciamento de recursos.
9. Na guia **Review+Create**, verifique o resumo de configuração e clique em **Create** para configurar o DDMC.

Como implementar o DDMC na Google Cloud Platform (GCP)

Como implantar o DDMC no GCP Marketplace

Etapas

1. Faça log-in no console do GCP Marketplace em https://cloud.google.com/marketplace.
2. Clique no botão **Conheça o Marketplace**. Na barra de pesquisa, digite **PowerProtect DD Management Center**.
3. Localize o produto e clique em **LAUNCH** para iniciar a implementação.
4. Forneça as seguintes informações: o nome do DDMC (o **Deployment name**, também o nome da instância), a **Zone** onde o VPC e a sub-rede são criados e selecione a **DDMC version**.
5. Selecione a **Network** e **Subnetwork**. Essas configurações são as padrão:

6. Selecione as regras de firewall. Essas configurações são as padrão:

7. Analise as informações e depois clique em **Deploy**.
8. Localize o PowerProtect DD Management Center implementado na página Instâncias do VM.

Implementar sistemas DDVE

Introdução

O DDMC fornece novas APIs REST para automatizar o gerenciamento do ciclo de vida dos sistemas DDVE em execução no Amazon Web Services (AWS).

As APIs de gerenciamento do ciclo de vida do DDVE permitem integrar DDVEs baseados em nuvem a seus sistemas de operações em nuvem. As APIs permitem:

- Gerenciar com segurança credenciais do AWS.
- Implementar instâncias do DDVE.
- Provisionar armazenamento EBS para o file system.
- Certificar-se de que DDVEs sejam consistentemente implementados.
- Desprovisionar e destruir DDVEs quando não forem mais necessários.

Instalação e pré-requisitos

A implementação de APIs do DDVE são fornecidas como parte do DDMC. O DDMC é executado como uma máquina virtual, separada dos DDVEs e sistemas DD que está gerenciando. O DDMC pode ser executado em hipervisores no local (ESXi, vCloud, Hyper-V ou KVM) ou como uma VM no AWS ou no Azure. Consulte o guia de instalação do DDMC para obter detalhes.

Para que o DDMC gerencie os DDVEs na nuvem, ele requer um acesso de rede não bloqueado para chamar as APIs do AWS e as APIs do DDVE (porta 3009 no DDVE, acessada via HTTPS).

DDVEs exigem uma licença para incluir e restaurar dados. Em vez de instalar arquivos de licença individuais, o DD DDMC configurará DDVEs usando um servidor de licenças. Você precisa instalar um servidor de licenças e configurar o DDMC para saber mais sobre o servidor. Você também precisa instalar um arquivo de licença de servidor no servidor de licenças com capacidade suficiente para sua implementação pretendida.

Gerenciando credenciais do Amazon Web Services (AWS)

Para implementar DDVEs e provisionar o armazenamento, o DDMC precisa ser capaz de chamar APIs do AWS. O AWS requer que um chamador de API apresente credenciais para autenticar o chamador antes de executar a API.

Para evitar problemas de segurança, o DDMC tem duas maneiras de acessar as credenciais do AWS. O primeiro método e o mais seguro é executar o DDMC como uma máquina virtual do AWS. Se você configurar o DDMC com as permissões AmazonEC2FullAccess, AmazonS3FullAccess e IAMFullAccess, isso permite ao DDMC chamar as APIs do AWS usando um conjunto de credenciais temporárias.

Se não puder usar credenciais baseadas em função, você pode criar um perfil de acesso. O perfil de acesso armazena com segurança a chave pública e chave secreta do AWS no banco de dados do DDMC. Quando um usuário invocar a API de implementação do DDVE, o DDMC usa o conjunto nomeado de credenciais para implementar o DDVE e provisionar o armazenamento. Você pode criar quantos perfis de acesso achar necessário, na URI /rest/v1.0/system/vi/access-info. Você opera em perfis de acesso usando as operações padrão POST, PUT, GET e DELETE.

Preparar a imagem de máquina Amazon do DDVE

Antes de implementar um DDVE, você deve criar uma imagem de máquina Amazon (AMI). O código do DDVE é fornecido como um arquivo de disco virtual VMware (VMDK). A Amazon tem ferramentas para converter esse arquivo em uma AMI. Em resumo, você transfere a imagem de disco de inicialização do DDVE para um bucket S3 e usa as ferramentas da Amazon para converter esse arquivo em uma AMI. Quando terminar, a AMI receberá a atribuição de um AMI ID. Você precisa desse ID como parte do processo de implementação.

Gerenciando recursos virtuais

Você pode implementar muitos DDVEs usando o mesmo conjunto de recursos de hardware. Com o DDMC, você pode criar um conjunto de recursos que serão usados em todas as implementações para manter a consistência. Esse objeto é chamado de perfil de recursos. No AWS, o perfil de recursos especifica:

1. A região do AWS, como "us_east_1"
2. O nome da AMI a ser usada para as implementações
3. O ID de sub-rede do AWS
4. O grupo de segurança do AWS

Consulte a documentação da AWS para obter mais informações sobre a região, o ID da sub-rede, o grupo de segurança e o ID da AMI. O ID do AMI é o ID que obtido ao criar a AMI do DDVE Perfis de recursos são gerenciados pela URI /rest/v1.0/system/vi/resource.

Criar um modelo de configuração do DDVE

O processo de implementação aplica um modelo de configuração a um DDVE recentemente implementado. O modelo de configuração define um conjunto de configurações do DD OS que deseja aplicar consistentemente a seus sistemas Data Domain ou PowerProtect. O modelo é armazenado no banco de dados do DDMC. O modelo de configuração tem seções para configurações de rede, notificação de alerta, configurações de hora, DD Boost, entre outros.

Para criar um modelo de configuração, você deve primeiro implementar um sistema Data Domain ou PowerProtect, configurá-lo e testá-lo, então extrair um modelo desse sistema. Crie modelos de configuração usando a API POST /rest/v1.0/system/config/templates, passando um nome para o modelo e o nome de um sistema Data Domain ou PowerProtect do qual extrair o modelo. Consulte o Apêndice B.

Implementar um DDVE

Depois de todas as etapas de preparação, você estará pronto para implementar um DDVE. Durante a implementação de um DDVE, o DDMC executa um workflow com várias etapas. As etapas do workflow são as seguintes:

1. Criação e inicialização de uma máquina virtual do AWS usando o AMI do DDVE.
2. Provisionamento de volumes do EBS para comportar os dados do file system e a conexão dos volumes ao DDVE.
3. Configuração do DDVE para usar um servidor de licenças.
4. Configuração do DDVE, hostname, endereço IP e a senha do sysadmin.
5. Criação de um file system do Data Domain ou PowerProtect nos volumes EBS.
6. Aplicação de um modelo de configuração opcional.
7. Adição do DDVE ao inventário do DDMC.

Inicie o processo executando um POST para /rest/v2.0/dd-systems. Esta é uma API atualizada para esta versão. O corpo da solicitação inclui uma nova estrutura que instrui o DDMC a implementar um DDVE. A estrutura de solicitação é semelhante a esta:

```
POST /rest/v2.0/dd-systems
{
```

```
    "hostname": "my-ddve-hostname",
    "password": "abc123",
    "deploy_info": {
        "environment": "aws",
        "common_deploy_info": {
            "vm_name": "my-ddve-name",
            "access_profile_name": "aws_access_profile",
            "resource_profile_name": "resource_profile",
            "config_template": "configuration_template_name"
        },
        "aws_specifc_deploy_info": {
            "init_config": 2,
            "max_config": "8TB"

        }
    }
}
```

Consulte a documentação on-line do REST para ver a explicação dos campos. Os valores legais e AWS e as descrições são conforme segue.

Tabela 7. AWS, valores legais e descrições

Campo	Valores legais	Descrição
init_config	Número inteiro sem sinal entre 1 e o tamanho máximo configurado	Capacidade do file system quando inicialmente implementado, em TiB.
max_config	16 TB, 32 TB, 96 TB e 256 TB	A capacidade máxima permitida do file system; todos os DDVEs são provisionados e licenciados com uma licença de avaliação de 500 GiB

Esse processo leva alguns minutos para ser concluído. Verifique se o tempo de espera excedido do client REST é longo o suficiente.

Enquanto a implementação estiver em execução, você pode monitorar seu andamento executando um GET no URI /rest/v1.0/tasks para visualizar uma lista de todas as atividades (ou as ativas). Na lista de tarefas, você pode recuperar um ID da tarefa e usar esse ID para GET /rest/v1.0/tasks/{ID} para obter o status detalhado da tarefa em execução.

Gerenciar uma DDVE

Depois que o DDVE for implementado, você poderá monitorá-lo e gerenciá-lo usando todas as interfaces padrão do DDMC. Você pode monitorar o status, integridade, capacidade e muito mais pela GUI do DDMC. Você pode iniciar o System Manager para fazer alterações no DDVE. Além disso, há várias APIs REST DDMC que você pode usar para fazer coisas como provisionar MTrees, criar exportações NFS, criar seus próprios aplicativos de monitoramento do desempenho e executar funções de exclusão/implementação. Consulte o Apêndice B.

Destruir um DDVE

Quando não precisar mais do DDVE, use a API DELETE /rest/v1.0/dd-systems/{SYSTEM-ID} para remover o DDVE do inventário do DDMC. Além de remover o sistema do inventário, o DDMC destruirá o DDVE e desprovisionará o armazenamento EBS usado para o file system. Novamente, essa é uma tarefa duradoura que você pode monitorar usando as URIs /rest/v2.0/tasks. Consulte o Apêndice B.

Ligar o DDMC

Sobre esta tarefa

Se a instalação for bem-sucedida, você poderá ligar a máquina virtual do DDMC e fazer log-in no sistema.

Etapas

1. Abra o Client e navegue até o local onde configurou o DDMC.
2. Clique com o botão direito do mouse na instância e selecione **Power On**.

3. Como opção, clique com o botão direito do mouse em **Console** para visualizar o processo de inicialização. Depois que uma sequência de inicialização for concluída com sucesso, um prompt da CLI é exibido. Você pode fazer log-in como **sysadmin** com a senha inicial **changeme**.

   NOTA: Embora a CLI possa ser usada para fazer log-in no DDMC e executar algumas operações (consulte "Diferenças entre a CLI do DDMC e a CLI do DDOS na página 135"), a interface preferencial para se trabalhar com o DDMC é a GUI.

Fazendo log-in e log-out no DDMC

O DDMC é acessado usando um navegador compatível em uma estação de trabalho que tenha acesso de rede à instância do DDMC. O DDMC dá suporte a vários usuários simultâneos.

Tabela 8. Navegadores compatíveis

Microsoft Windows 8 e 10	Apple OS X
Microsoft Edge	--
Google Chrome (versão mais recente)	Google Chrome (versão mais recente)
Mozilla Firefox (versão mais recente)	Mozilla Firefox (versão mais recente)

Outras versões de navegador também podem funcionar. Essas versões específicas foram validadas. Consulte as notas da versão para obter as informações mais atualizadas.

Fazer log-in no DDMC

O log-in inicial requer o uso do ID do usuário "sysadmin" e da senha "changeme" (a senha padrão). Em seguida, será solicitado que você altere a senha do sysadmin. Depois disso, outros usuários com diferentes funções (que foram adicionados ao DDMC) podem fazer log-in.

Sobre esta tarefa

Faça log-in no DDMC.

Etapas

1. Abra um navegador e digite o nome do host ou endereço IP do DDMC.

   O link **Secure Login** é fornecido para estabelecer uma conexão segura pela rede usando HTTPS em vez de HTTP. Essa opção utiliza um certificado autoassinado por padrão, o qual o usuário deve aceitar, apesar de avisos do navegador.
2. Na janela de log-in, digite um nome de usuário e senha e pressione Enter ou selecione **Log In**.

Resultados

Após fazer log-in no DDMC, o painel de controle é exibido, mostrando o conjunto padrão de recursos de monitoramento.

Conceitos relacionados

Gerenciar o acesso do usuário local ao DDMC na página 105
Ícones e controles globais na página 130

Fazendo log-in com certificados de Public Key Infrastructure (PKI) e de cartão de acesso comum (CAC)

Os usuários podem fazer log-in no DDMC com seu PKI/CAC existente e apresentar um certificado de autenticação ou autorização ao sistema Data Domain ou PowerProtect.

Pré-requisitos

O log-in com um certificado só está disponível por meio de uma página de log-in seguro (HTTPS), e também requer uma importação do certificado de raiz da Autoridade de Certificação (CA) e de arquivos intermediários por meio da CLI.

Etapas

1. Para importar a raiz de CA, digite o seguinte comando na CLI do Windows ou Linux:
   `ssh sysadmin@DDMC adminaccess certificate import ca application login-auth < rootCA.crt`
2. Para importar os arquivos intermediários da Autoridade de Certificação, digite o seguinte comando na CLI:
   `ssh sysadmin@DDMC adminaccess certificate import ca application login-auth < intermediateCA.crt`
3. Selecione o link "Log-in com certificado".
   A caixa de diálogo **Select a Certificate** é exibida, permitindo que os usuários selecionem o certificado apropriado para usar para fazer log-in DDMC.

   NOTA: Somente os usuários que existem no DDMC serão exibidos.

   - O certificado é compatível com usuários locais, NIS e AD.
   - Os usuários são autenticados pelo sistema Data Domain ou PowerProtect usando o certificado público presente no CAC/PKI.
   - Usar um cartão CAC/PKI pode exigir que o usuário digite o PIN como parte do processo de autenticação de certificado.

Fazer log-out do DDMC

Para fazer log-out do DDMC, clique no ícone de usuário no banner do DDMC e selecione **Logout** na lista suspensa ou apenas feche a janela do navegador.

Adicionar (registrar) sistemas ao DDMC

Antes de poder gerenciar um sistema DD no DDMC, você deve adicioná-lo (registrá-lo) ao inventário. Uma única instância do DDMC pode ter um máximo de 150 sistemas adicionados. Grupos de até 20 sistemas podem ser registrados ao mesmo tempo.

Etapas

1. Selecione **Inventory** > **Systems**.
2. Clique em **ADD** (sinal de mais verde). Digite o seguinte para o primeiro sistema e, em seguida, selecione Add para continuar adicionando sistemas (até 20 sistemas no total). Certifique-se de que a caixa ao lado do sistema a ser adicionado esteja marcada.
   - Selecione **System** ou **HA system**.
   - **Host name** (obrigatório) — digite o nome de host completo (use caracteres alfanuméricos, traços, pontos e sublinhados) ou o endereço IP. Certifique-se de que o nome do host e o nome DNS do sistema correspondam; uma disparidade pode causar problemas com o software para backup.

     NOTA: Para sistemas de alta disponibilidade, especifique o nome de host flutuante; caso contrário, a operação de adição falhará.
   - **Sysadmin password** (obrigatório) — digite a senha do sysadmin usada no sistema Data Domain ou PowerProtect (obrigatório).
   - **Proxy Firewalls** (opcional) — digite o nome do host do proxy de entrada e de saída (ou endereço IP) e o número da porta a ser usada pelo firewall. Se essa opção estiver selecionada e você não alterar o número da porta, o padrão (3009) será usado. Se você alterá-lo, o número da porta deverá ser entre 1 e 65535. As configurações da porta padrão permitem que o DDMC se comunique com o sistema. Se as portas tiverem sido alteradas no firewall ou no sistema, elas também deverão ser atualizadas aqui.

     NOTA:

     - Os firewalls de proxy não são compatíveis com sistemas de alta disponibilidade, portanto, esta seção não é editável ao adicionar um sistema de alta disponibilidade.
     - Para obter informações mais detalhadas, consulte a seção Números de porta e nomes do host do proxy de entrada e de saída usados pelo firewall na página 36.
   - **Certificate** (opcional) — verifique as informações do certificado clicando nas células associadas. O nome do assunto no certificado CA do DDMC deve corresponder ao nome do host do DDMC ou o SSL falhará na verificação do host.

     NOTA: Para ambientes que usam certificados SHA-256 autoassinados, os certificados devem ser gerados novamente manualmente depois que o processo de atualização for concluído, uma relação de confiança deve ser restabelecida com os sistemas externos que se conectam ao sistema.
   - **Progress** — mostra a porcentagem concluída, conforme o sistema está sendo adicionado.
   - **Takeover managed system** — marque essa caixa de seleção se o sistema for gerenciado por outro DDMC. O sistema se tornará não gerenciado, mas não será removido do outro DDMC.
3. Clique em **REGISTER** para continuar.

Resultados

Uma barra de progresso é exibida na página mostrando o progresso da sincronização inicial de dados para os sistemas DD adicionados recentemente. Além disso, os detalhes do progresso do trabalho podem ser rastreados na página **Health** > **Jobs**.

NOTA: Em caso de falha, selecione **Get failure reason** na barra de progresso. Depois de corrigir o motivo do problema, clique em **REGISTER** para registrar novamente.

Depois que um sistema é adicionado ao DDMC, todas as informações históricas desse sistema são copiadas para o DDMC. A partir desse ponto, sempre que os dados operacionais forem alterados no sistema, o sistema notifica o DDMC, que imediatamente consulta o sistema para receber essas novas informações.

Causas comuns de erros durante a adição de sistemas

A seguinte lista de verificação pode ajudá-lo a resolver alguns erros que podem ocorrer ao tentar adicionar um sistema ao DDMC:

- Certifique-se de que o sistema esteja on-line. Um sistema deve estar on-line para ser adicionado ao DDMC.
- Se você tiver especificado um número da porta nas configurações de firewall do proxy, certifique-se de que ele esteja correto.
- Certifique-se de que não haja nenhum problema de rede impedindo a comunicação entre o DDMC e o sistema.
- Se você especificou um nome do host para o sistema, verifique se ele pode ser resolvido no namespace (DNS ou lista de host).
- Certifique-se de que a senha digitada no sistema esteja correta.
- Certifique-se de que a versão do DDOS do sistema seja compatível com a versão atual do DDMC.
- Certifique-se de que o sistema já não seja gerenciado por outro DDMC. Para resolver esse problema, você pode excluir o sistema do DDMC original ou selecionar a caixa de seleção **Takeover managed system**. O sistema será adicionado ao novo DDMC, mas o status do sistema será alterado para unmanaged no DDMC original e a coleta de dados será suspensa para esse sistema.
- Para sistemas de alta disponibilidade, certifique-se de que:
  - O nome de host especificado não seja o nome de host do nó em espera.
  - O sistema de alta disponibilidade não esteja no modo degradado.
  - Ambos os nós estão funcionando.

Editando as configurações do sistema

Depois que forem adicionados sistemas DD ao DDMC, você pode editar suas definições de configuração, propriedades, atribuições de grupos e limites.

Etapas

1. Selecione **Infrastructure** > **Systems**.
2. Selecione um ou mais sistemas e, em seguida, EDIT (lápis amarelo).
3. Na caixa de diálogo **Edit System**, escolha uma ou todas as guias para fazer alterações (selecione **APPLY** ou altere as guias para salvar as novas configurações e continuar a reconfiguração). Se você tiver selecionado mais de um sistema, somente as guias Properties e Thresholds estarão disponíveis.
   - **Configuration** permite que você edite o nome do host do proxy de entrada e de saída (ou endereço IP) e o número da porta usado pelo firewall. Se essa opção estiver selecionada e você não alterar o número da porta, o padrão (3009) será usado. Se você alterá-lo, o número da porta deverá ser entre 1 e 65535. As configurações da porta padrão permitem que o DDMC se comunique com o sistema. Se as portas tiverem sido alteradas no firewall ou no sistema, elas também deverão ser atualizadas aqui.

     NOTA: Configuration não é exibido para sistemas de alta disponibilidade.

     NOTA: Para obter mais informações, consulte a seção anterior, Números de porta e nomes do host do proxy de entrada e de saída usados pelo firewall na página 36.
   - **Properties** permite que você edite informações para classificação de sistemas e os dados contidos em contextos de replicação e MTrees, para pesquisar, filtrar e organizar. Se você tiver selecionado mais de um sistema e houver valores diferentes para essa propriedade nos diferentes sistemas, o campo exibe *Mixed values*. Se você alterar o valor, todos os sistemas receberão o novo valor. Existem propriedades padrão e criadas pelo usuário (**Administration** > **Properties** > **System**). As propriedades padrão de Model, sistema operacional e Domain Name não podem ser editadas. Data Center é uma propriedade "híbrida" do tipo string de valor fixo. Por ser uma propriedade padrão do sistema, ele não pode ser excluído, mas seus valores podem ser editados e definidos para um sistema.
   - **Groups** permitem que você organize os sistemas com um nome específico, em uma estrutura hierárquica criada pelo administrador do DDMC, que é útil para pesquisas. Você pode adicionar ou remover atribuições do grupo e selecionar ou apagar a seleção de atribuições do grupo para o sistema. Qualquer quantia de grupos e subgrupos pode ser selecionada.
   - **Thresholds** indicam os limites de capacidade de advertência e crítica e são exibidos nos modos de exibição de capacidade e nos relatórios. Use o controle deslizante para especificar limites como uma porcentagem da capacidade total. Ao editar vários sistemas

com os limites de advertência mistos, o valor inicial de advertência é zero. Ao editar vários sistemas com limites críticos mistos, o valor crítico inicial é 100. Se você alterar o valor, todos os sistemas receberão o novo valor.

4. Selecione **OK** para salvar e sair da reconfiguração do sistema.

Modelos de configuração

Os modelos de configuração permitem que um administrador do DDMC crie um modelo para a configuração de um sistema Data Domain ou PowerProtect.

Esta função permite:

- Que a mesma configuração seja aplicada a vários dispositivos.
- Uma configuração válida e reconhecida de um sistema DD para usar como modelo padrão.
- Monitoramento de vários sistemas para conformidade de configuração e alterações de auditoria, incluindo quem as fez e quando.

NOTA: Um modelo de configuração baseia-se na configuração de um sistema de origem e não pode ser criado a partir do zero no DDMC.

Os detalhes do modelo podem ser visualizados clicando no botão Detalhes na linha da tabela. Para obter detalhes adicionais sobre configuração, clique em **Exibir detalhes da configuração** no painel de detalhes no lado direito.

Criar modelo de configuração

1. Selecione **Infrastructure** > **Configuration Templates**.
2. Clique em **Create**.
3. Nomeie o modelo (obrigatório).
4. Selecione o sistema de configuração de origem em uma lista de sistemas existentes gerenciados pelo DDMC.

   NOTA: O sistema de origem deve estar on-line e possível de ser acessado.
5. Marque ou desmarque qualquer recurso ou sub-recurso.
6. Clique em **Create Template**.

Excluir modelo de configuração

1. Selecione **Infrastructure** > **Configuration Templates**.
2. Selecione o modelo de configuração a ser excluído.
3. Clique em **Delete**.
4. Na caixa de diálogo **Delete Templates**, clique em **YES** para confirmar a exclusão.

NOTA: A exclusão de um modelo também exclui todos os agendamentos de auditoria associados, mas não é possível excluir modelos com histórico de auditoria.

Aplicar modelo de configuração

NOTA: Somente os sistemas on-line são mostrados na lista Available Systems para aplicar um modelo.

1. Selecione **Infrastructure** > **Configuration Templates**.
2. Selecione o modelo de configuração a ser aplicado.
3. Clique em **Apply**.
4. Pesquise em Select Systems e selecione um ou mais sistemas na lista Available Systems para o modelo a ser aplicado.
5. Clique em **Add**.
6. Clique em **Next**.
7. Clique em **Apply**.

Modelo de configuração de auditoria

Uma auditoria gera um alerta para cada sistema que não conforme.

1. Selecione **Infrastructure** > **Configuration Templates**.

2. Selecione o modelo de configuração a ser auditado na guia Templates.
3. Clique em **Audit**.
4. Pesquise em Select Systems e selecione um ou mais sistemas na lista de Available Systems para auditar.
5. Clique em **Add**.
6. Clique em **Next**.
7. Revise a página de resumo e clique em **Audit**.

Um link direto para o status do trabalho fica disponível. O status também pode ser visualizado indo para **Health** > **Jobs**.

Agendamentos de auditoria

1. Selecione **Infrastructure** > **Configuration Templates**.
2. Selecione a guia **Audit Schedules** e clique em **Create**.
3. Defina o agendamento adicionando:
   - Nome
   - Frequência (Diária ou semanal)
   - Data de início
   - Hora
   - Modelo (a partir da lista de modelos de configuração disponíveis)
4. Pesquise em Select Systems e selecione um ou mais sistemas na lista de Available Systems para auditar.
5. Clique em **Add**.
6. Clique em **Next**.
7. Revise a página de resumo e clique em **Create**.

Histórico de auditoria

A guia **Audit History** pode ser acessada navegando em **InventoryConfiguration Templates**. É exibida uma tabela com nome do sistema, nome do modelo, nome do agendamento, data de execução da auditoria, status do trabalho de auditoria, status de conformidade e recursos não compatíveis.

Clique em **Template Name** para obter detalhes de configuração.

Se um número diferente de zero for mostrado na coluna Non-Compliant Features, clique no numeral para ver os recursos não conformes específicos.

Atribuindo propriedades

O procedimento para atribuir uma propriedade varia, dependendo de onde a propriedade é usada: sistema ou replicação.

Tarefas relacionadas

Adicionando propriedades a sistemas e pares de replicação na página 28

Atribuindo valores de propriedade do sistema

Depois de adicionar uma propriedade a um sistema Data Domain ou PowerProtect (**Administration** > **Properties** > **System**), você pode atribuir valores a essa propriedade.

Etapas

1. Selecione **Infrastructure** > **Systems**.
2. Selecione um ou mais sistemas.
3. Selecione **EDIT** (lápis amarelo) e, na caixa de diálogo **Edit System**, selecione a guia **PROPERTIES**.

   Data Center é a propriedade padrão que deve aparecer ao se adicionar um sistema.
4. Para cada propriedade listada, atribua um valor. Se você tiver selecionado mais de um sistema e os sistemas tiverem diferentes valores para essa propriedade, o campo exibirá *Mixed values*. Se você alterar o valor, todos os sistemas receberão o novo valor. Um controle **Undo** é fornecido para desfazer a configuração e um controle **More Details** mostra os valores salvos para cada sistema selecionado. Para as propriedades que foram criadas como:

- String — digite o texto que é exibido como o valor.
- Boolean — selecione um dos dois valores na lista drop-down.
- Fixed-value string (e multi-value) — selecione o valor na lista drop-down.

5. Clique em **OK** para definir os valores.

Tarefas relacionadas

Atribuindo valores de propriedade de replicação na página 28
Adicionando propriedades a sistemas e pares de replicação na página 28

Atribuindo valores de propriedade de replicação

Depois de adicionar uma propriedade de pares de replicação (**Administration** > **Properties** > **Replication**), você pode atribuir valores a essa propriedade.

Etapas

1. Selecione **Replication** > **Automatic**.
2. Selecione um par de replicação.
3. Selecione **ASSIGN PROPERTIES** e defina um valor. Para as propriedades que foram criadas como:
   - String — digite o texto que será exibido como o valor.
   - Boolean — selecione um dos dois valores na lista drop-down.
   - Fixed value string (e multi-value) — selecione o valor na lista drop-down.
4. Clique em **ASSIGN** para definir os valores.
5. Para ver os valores atribuídos a contextos de replicação, você pode adicionar essa propriedade como uma coluna na tabela de replicação na página Automatic replications:
   a. Selecione o ícone Show Columns.
   b. Selecione a caixa de seleção da propriedade na lista.
   c. Você verá o nome da propriedade como o título da coluna, e qualquer valor atribuído a um contexto aparecerá na célula.

Tarefas relacionadas

Atribuindo valores de propriedade do sistema na página 27
Adicionando propriedades a sistemas e pares de replicação na página 28

Adicionando propriedades a sistemas e pares de replicação

Properties apresentam informações de classificação de sistemas e os dados contidos em contextos de replicação para pesquisar, filtrar e organizar. Por exemplo, você pode atribuir propriedades para ajudar a filtrar a lista de sistemas na página **Infrastructure** > **Systems** e restringir o escopo de resultado produzido por um recurso do painel de controle ou relatório gerado. Quando um sistema é adicionado ao DDMC, um conjunto de propriedades de administração padrão (modelo do sistema, versão do DDOS, nome do domínio e datacenter) é adicionado automaticamente. Você pode adicionar e atribuir outras propriedades, conforme necessário.

Etapas

1. Selecione **Administration** > **Properties**.
2. No canto superior direito, selecione uma das guias (System ou Replication) e selecione **ADD** (sinal de adição verde).
3. Na caixa de diálogo Add Property, digite um nome para a propriedade e selecione seu tipo de operação:
   - **String** — permite que uma string de até 256 caracteres seja configurada ao atribuir a propriedade, por exemplo, você pode nomear a propriedade "Comments" e um usuário pode digitar "Aguardando resposta de Tom", "Ainda não está pronto", como exemplos.
   - **Boolean** — cria uma condição na qual é possível atribuir um destes dois valores, por exemplo, você pode nomear a propriedade "Restored?" e os valores possíveis podem ser "True", "False", "Yes" ou "No".
   - **Fixed-value String** — permite que você forneça um nome e valores específicos para a propriedade, por exemplo, "Department" pode ser o nome e "Finance", "Human Resources", "Marketing" podem ser os valores. A seleção da opção **Allow multiple types** permite que você atribua mais de um valor.
4. Clique em **ADD**.
5. Atribua valores para as propriedades, conforme descrito em "Assigning Properties".

Conceitos relacionados

Atribuindo propriedades na página 27
Exibindo informações de propriedade na página 38

Tarefas relacionadas

Atribuindo valores de propriedade do sistema na página 27
Atribuindo valores de propriedade de replicação na página 28
Exibindo propriedades de um elemento na página 38
Localizando elementos por valor de propriedade na página 39

Continuar a configuração do DDMC

Você concluiu a configuração básica do DDMC e está pronto para usá-lo.

A configuração básica permite que o DDMC seja iniciado, mas talvez seja preciso definir muitas outras configurações para integrar totalmente o DDMC ao seu site.

Pode ser necessário definir as configurações de rede e as tabelas de roteamento, definir a configuração de fuso horário e fornecer acesso aos usuários. Todas essas informações estão descritas no capítulo Executando configuração adicional.

Noções básicas sobre o RBAC no DDMC

O DDMC utiliza o controle de acesso baseado em função (RBAC) para controlar como os dados são manipulados e exibidos no DDMC e nos sistemas Data Domain gerenciados pelo DDMC.

Os usuários do DDMC podem:

- Ter uma de três funções no DDMC: *admin* (administrador do sistema), *limited-admin* (administrador limitado) ou *user* (usuário básico)
- Ter uma das quatro funções nos sistemas gerenciados pelo DDMC: *admin* (administrador do sistema), *limited-admin* (administrador limitado), *user* (usuário básico) ou *backup operator* (operador de backup)
- Modificar os estados do DDMC apenas se tiverem a função *admin* ou *limited-admin*
- Exibir dados de um sistema (pelo DDMC), conforme permitido pela função que possuem no sistema Data Domain
- Modificar um sistema apenas se tiver a função *admin* ou *limited-admin* no sistema Data Domain ou PowerProtect

Visualizando os elementos da página do DDMC

A página do DDMC é composta por vários elementos.

As três áreas principais da página principal do DDMC são o banner, o painel de navegação e o ambiente de trabalho.

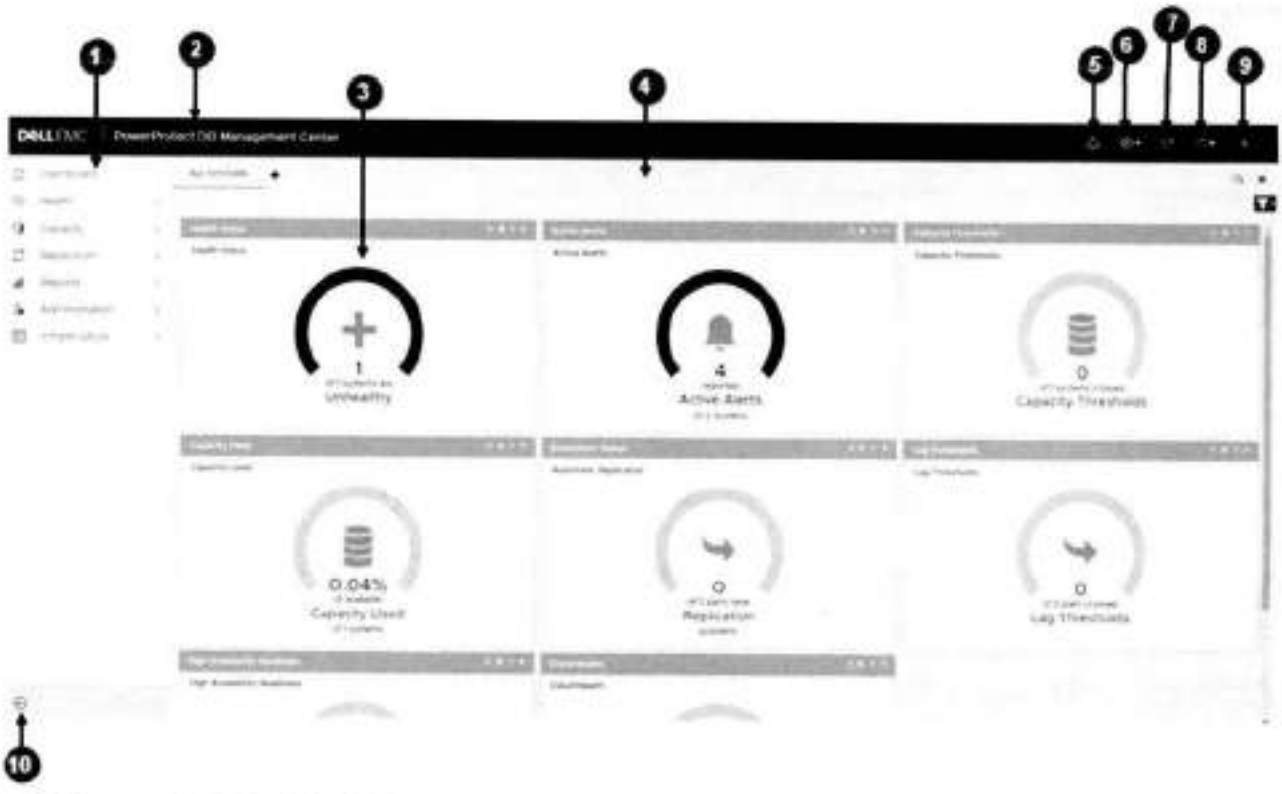


Figura 1. Elementos da página do DDMC

1. Painel de navegação com a lista de módulos
2. Banner com status e área de controle
3. Recurso de painel de controle
4. Ambiente de trabalho
5. Alerts
6. Configurações

   NOTA: As configurações são exibidas em um menu suspenso para usuários administradores e administradores limitados com uma nova opção de **Pacotes de suporte**.
7. Atualizar
8. Controle de ajuda on-line
9. Perfil do usuário

   NOTA: Um ícone circular é exibido com a primeira letra alfabética do ID do usuário. Passe o mouse sobre o círculo para mostrar uma pequena dica de ferramenta com o texto "Configurações do usuário".
10. Menu recolher ou expandir.

O painel de navegação é organizado por módulo: Dashboard, Health, Capacity, Replication, Reports, Administration e Inventory. Dentro de cada módulo, você pode selecionar o nome de uma página de assunto a ser exibida no ambiente de trabalho.

A menos que o painel esteja maximizado, o banner ficará sempre visível. Ele fornece controles para filtrar o escopo da página ativa do ambiente de trabalho (o controle do filtro é exibido somente nas páginas de monitoramento), para abrir a ajuda on-line e para fazer log-out.

O banner mostra as notificações de alerta (que você pode selecionar para ver uma janela de caixa de diálogo informativa com um link para a página de Alertas) e fornece o usuário ativo, a função e o acesso à exibição clássica do DDMC.

Os controles globais padrão (adicionar, editar e excluir) permitem a interação com o aplicativo e gerenciam como as informações são exibidas nas páginas com tabelas (classificando o conteúdo da coluna por meio de controles em ordem crescente ou decrescente e ocultar ou exibir colunas).

Tarefas relacionadas

Trabalhando com filtros na página 40

Acessando uma página do DDMC

Os elementos de navegação das páginas do DDMC mudam o foco e o escopo do conteúdo exibido no ambiente de trabalho.

Sobre esta tarefa

Figura 2. Acesso à página do DDMC

1. Os tópicos do módulo são encontrados à esquerda, no painel de navegação.
2. Os botões de alternância (se aplicável) permitem que você mude de uma lista padrão do sistema para um grupo de sistemas, para uma exibição de tenant, etc. Se você escolher grupos, somente os grupos criados serão exibidos. Nesse figura, você pode escolher entre exibição de **Systems** ou **Groups**.

Tarefas relacionadas

Trabalhando com filtros na página 40

Organizando o painel de controle

O painel contém *widgets* que você cria em um conjunto de funções de monitoramento. O painel permite que você verifique rapidamente condições importantes, como sistemas inacessíveis, alertas ativos, diminuição de capacidade, etc.

Você pode configurar guias separadas no painel de controle e incluir recursos específicos para cada uma dessas guias. Usos sugeridos para guias são organizar um conjunto de sistemas baseados na lista de membros do grupo, local, versão do sistema operacional, tipo de dados, etc. Outra sugestão é organizar por tipo de recurso, por exemplo, uma guia contendo recursos Current Health Status para todos os sistemas.

Por padrão, a cada usuário é atribuído um painel com uma guia, preenchido por cada um dos recursos fornecidos, configurado para abranger todos os sistemas que o usuário estiver monitorando. Você pode modificar, adicionar a ou até mesmo excluir a guia padrão do painel.

Uma guia com todos os seus recursos pode ser copiada para uma nova guia e depois editada.

Adicionando e configurando guias

As guias podem ser criadas rapidamente clicando no sinal de mais azul (+) no banner e preenchendo os campos obrigatórios **Name** e **Filter** na janela **Add Dashboard**. Para personalizar sua configuração do DDMC Management Center, você pode adicionar guias escolhendo um nome exclusivo, o número de colunas e posicionamento.

Etapas

1. Selecione **Home** > **Dashboard**.
2. No painel de controle, selecione o controle **Add tab** no banner, no canto superior direito.
3. Na caixa de diálogo **Add and Configure Dashboard Tabs**, selecione **ADD** (sinal de mais verde).
4. No campo de texto selecionado, digite o nome da guia.
5. Escolha o número de colunas para a guia (mais colunas produzem recursos menores) e qualquer filtro aplicável.
6. Clique em **ADD**.
7. Solicite o posicionamento da guia no painel de controle usando os controles **MOVE UP** ou **MOVE DOWN**.
8. Clique em **SAVE**.

Resultados

A nova guia será exibida no painel de controle.

Adicionando recursos

Você também pode adicionar recursos para personalizar a configuração de seu DD Management Center.

Etapas

1. Selecione **Home** > **Dashboard**.
2. No painel de controle, navegue até uma guia (All Systems, etc.) ou crie uma nova guia (consulte a seção anterior).
3. Selecione o controle **Add widget** no banner, no canto superior direito.
4. Na caixa de diálogo **Add Dashboard Widget**, digite um nome que reflita o uso do recurso. Por exemplo, usando um modelo de Lag Thresholds, é possível nomear o recurso de "New Jersey Lag Thresholds", se você definiu filtros para mostrar apenas os sistemas que replicam para Nova Jersey. O nome deve ser exclusivo para esta guia.
5. Selecione um modelo para o resultado desejado. Ao selecionar um modelo, uma imagem é exibida em Example, mostrando um exemplo de um recurso desse tipo.
6. Se aplicável, na área Settings, selecione uma das opções disponíveis (como a de filtragem para restringir o escopo do monitoramento do recurso). Os recursos podem ser filtrados com o uso de primitivos de filtro padrão como sistemas, grupos e propriedades. Além disso, dependendo do modelo, pode haver outras configurações que você possa definir.
7. Clique em **ADD**.

Resultados

O novo recurso será exibido no painel de controle.

Modelos de recursos

Você pode adicionar, editar ou excluir os recursos do painel de controle, selecionando o controle Add widget no banner, no canto superior direito, usando o controle Edit widget no banner de cada recurso ou usando o controle Remove widget no banner de cada recurso, respectivamente.

Recurso Health Status

O recurso **Health Status** mostra um resumo de fatores de integridade importantes de sistemas monitorados, como status do file system, status de replicação, alertas e status de protocolo.

Se todos os sistemas estiverem íntegros, uma versão em verde do recurso será exibida, preenchendo o padrão de arco. Entretanto, se alguns dos sistemas estiverem não íntegros, seja em file system, replicação ou outras áreas, a proporção será mostrada no gráfico vermelho, e o número abaixo exibirá a contagem. A navegação deste recurso leva o usuário à página Health Status.

Selecione o controle Show detail (**>>**) para exibir a página **Health** > **Status**.

Recurso Active Alerts

O recurso **Active Alerts** mostra a distribuição de alertas ativos em todos os sistemas gerenciados por tipo: Emergency & Alert, Critical & Error e Warning.

Se não houver alertas para nenhum dos sistemas no inventário, o recurso exibirá um arco vazio, e a cor do texto será alterada para azul neutro. Os alertas de advertência são mostrados em amarelo. Alertas críticos ou acima são mostrados em vermelho. Se houver pelo menos um alerta, o arco ficará cheio. Ele funciona de modo similar a um gráfico de pizza. A navegação deste recurso leva o usuário à página Health Alerts.

Selecione o controle Show detail (**>>**) para exibir a página **Health** > **Alerts**, em que é exibida uma lista completa de alertas de integridade.

Recurso Capacity Thresholds

O recurso **Capacity Thresholds** mostra a distribuição de utilização da capacidade em todos os sistemas gerenciados.

Esse recurso mostra a contagem de sistemas que ultrapassaram os limites de capacidade. Se nenhum dos sistemas tiver ultrapassado o limite, o recurso exibe um arco vazio. Os sistemas que ultrapassaram o limite de advertência serão mostrados em amarelo, e os que ultrapassaram o limite crítico serão exibidos em vermelho. A navegação deste recurso leva o usuário à página Systems Capacity Thresholds.

Selecione o controle Show detail (**>>**) para exibir a página **Capacity** > **Systems**.

Recurso Capacity Used

O recurso **Capacity Used** mostra a proporção entre espaço usado e espaço disponível.

Esse recurso mostra a porcentagem total de capacidade usada. Uma vez que o recurso não representa um estado de integridade, o texto e a cor estão sempre em um estado neutro. O indicador mostra a proporção de capacidade usada em azul, e o texto é sempre azul. A navegação deste recurso leva o usuário à página Systems Capacity Thresholds.

Selecione o controle Show detail (**>>**) para exibir a página **Capacity** > **Systems**.

Recurso Replication Status

O recurso **Replication Status** mostra um resumo para pares de replicação e pares em cascata.

Esse recurso mostra uma contagem de sistemas com problemas de replicação. Se não houver problemas relacionados à replicação, o recurso exibirá um arco vazio. Se houver sistemas com problemas, o recurso mostrará a proporção dos problemas. A navegação deste recurso leva o usuário para a página de replicação sob demanda ou automática, dependendo do tipo de recurso que foi configurado.

Entre as opções de configuração, estão a configuração do recurso para monitorar replicações somente Automáticas ou somente Sob demanda.

Selecione o controle Show Details (**>>**), para exibir a página **Replication** > **Automatic**.

Recurso Lag Thresholds

O recurso **Lag Threshold** mostra a contagem de replicações com níveis crítico e de advertência, com base na Lag Threshold Policy.

Esse recurso mostra a contagem de pares que ultrapassaram os limites de intervalo. Se nenhum dos pares ultrapassar o limite, o recurso exibirá um arco vazio. Os pares que ultrapassarem o limite de advertência serão mostrados em amarelo, e os que ultrapassarem o limite crítico serão exibidos em vermelho. Se os limites de advertência e críticos forem ultrapassados para um par de replicação, o pior status (crítico) tem precedência.

Selecione o controle Show detail (**>>**) para exibir a página de replicação automática (**Replication** > **Automatic**), em que a lista de todas as replicações filtradas é exibida. A Lag Threshold Policy pode ser visualizada ou modificada a partir daqui.

Recurso High Availability Readiness

O recurso **High Availability Readiness** mostra um resumo do status de todos os sistemas de alta disponibilidade no inventário.

Esse recurso mostra o número total de sistemas de alta disponibilidade, o número de sistemas de alta disponibilidade que não estão prontos para failover e o número de sistemas de alta disponibilidade que estão prontos. Se houver qualquer sistema de alta disponibilidade que esteja não pronto para failover, o velocímetro mostra essa fração colorida em vermelho. Se todos os sistemas de alta disponibilidade estiverem prontos para failover, o velocímetro mostra tudo verde.

Os usuários podem filtrar por sistemas, grupos, propriedades e regras. O filtro por sistemas mostra apenas os sistemas de alta disponibilidade disponíveis no inventário.

A seleção do controle Show detail (**>>**) o direciona para a página **Health** > **Status**. Se houver sistemas de alta disponibilidade no inventário, essa navegação mostrará os sistemas filtrados pelos sistemas de alta disponibilidade.

Clicar no gráfico também navega até a **página Health Status**, filtrada por qualquer sistema de alta disponibilidade que não esteja pronto para failover. Se todos os sistemas estiverem prontos para failover, a navegação até a **página Health Status** do gráfico mostra uma lista de sistemas de alta disponibilidade.

Recurso Cloud Health

O recurso **Cloud Health** monitora a integridade da perspectiva do sistema habilitado para nuvem.

Uma nova opção de **Cloud Health** está disponível na caixa de diálogo **Add Dashboard Widget**, na opção suspensa **Template**. Ao selecionar a opção **Cloud Health**, é mostrada a imagem de visualização para o recurso Cloud Health. Esse recurso exibe a integridade de Cloud Tier de sistemas estendidos de Cloud no inventário. Filtros podem ser aplicados ao recurso **Cloud Health**, semelhante a todos os outros recursos do painel de controle. A opção Filter by System para o recurso Cloud Health mostra somente uma lista de sistemas estendidos de Cloud.

O monitoramento da integridade da unidade de nuvem é feito no nível de sistema no DDMC. A exibição Health Status indica o número de sistemas habilitados para a nuvem que estão Active (verde), Delete Pending and Disabled (amarelo), e Error and Disconnected (vermelho).

Quando Cloud Tier de cada sistema estendido de Cloud registrado com um DDMC está íntegro, o que significa que as unidades de Cloud nesses sistemas estão íntegras, o indicador é exibido em verde.

Clicar no indicador (ou na imagem dentro do recurso ou no botão Show Details (>>) na barra de ferramentas) vai para a página Health Status, filtrada pela lista completa de sistemas estendidos de Cloud.

Se um sistema tiver duas unidades de nuvem, uma no estado Delete Pending and Disabled e outra no estado Disconnected, o recurso será exibido em amarelo.

Quando Cloud Tier em algum ou em todos os sistemas estendidos de Cloud não estiver íntegro, o que significa que uma ou mais unidades de Cloud nesses sistemas não estão íntegras, o indicador mostrará a fração dos sistemas estendidos de Cloud cujo Cloud Tier não está íntegro. Se todos os cinco sistemas estendidos da nuvem não estiverem íntegros, todo o indicador estará em vermelho.

Clicar no indicador (ou na imagem dentro do recurso ou no botão Show Details (>>) na barra de ferramentas) vai para a página Health Status, filtrada pelos sistemas estendidos de Cloud que não estão íntegros.

Se uma unidade da nuvem estiver íntegra e outra com erros, o recurso deverá exibir **error** para o Cloud Tier e precisará de uma solução de problemas adicional para determinar a causa do erro e qualquer ação corretiva que possa ser tomada. O recurso exibirá um indicador com a proporção de erro em vermelho e o restante em cinza.

NOTA: O pior estado para as unidades da nuvem em um sistema tem prioridade.

Os usuários podem filtrar por sistemas, grupos, propriedades e regras. O filtro por sistemas mostra apenas os sistemas estendidos da nuvem disponíveis no inventário.

Copiando guias

Você pode criar uma guia que contenha os mesmos recursos que uma guia existente, copiando essa guia.

Etapas

1. Selecione **Home** > **Dashboard**.
2. Selecione o controle **Add tab** no banner, no canto superior direito.
3. Na caixa de diálogo **Add and Configure Dashboard Tabs**, selecione o nome da guia para copiar e, em seguida, **COPY**.
4. Na caixa de texto, digite o novo nome para a guia (digitando "COPY OF...").
5. Se quiser alterar o número de colunas, selecione o número atual e altere-o usando a lista drop-down.
6. Se quiser alterar a posição da nova guia, use as setas **MOVE UP** ou **MOVE DOWN**.
7. Clique em **SAVE**.

Resultados

A nova guia será exibida no painel de controle. Você pode abrir os recursos na nova guia para modificar suas propriedades.

Como editar guias

Você pode editar uma guia existente usando o ícone Filtro no canto superior direito.

Sobre esta tarefa

Clique no ícone Filtro para:

- Filtrar por grupo
- Filtrar por propriedade
- Filtrar por sistema
- Filtrar por regra

- Apagar o filtro

Como filtrar guias

As guias podem ser filtradas usando o ícone Filtro no canto superior direito.

Clique no ícone Filtro para:

- Filtrar por grupo
- Filtrar por propriedade
- Filtrar por sistema
- Filtrar por regra
- Apagar o filtro

Modificando recursos

Você pode modificar os recursos que foram copiados de uma guia como um ponto de partida para um novo conjunto. Por exemplo, é possível alterar as propriedades do filtro para monitorar um grupo, conjunto de sistemas ou regra diferente.

Para modificar um recurso, use o ícone Edit widget na barra de título do recurso e altere o nome, as configurações (se disponível) e a filtragem.

NOTA: Não é possível alterar o tipo de recurso (conforme determinado pelo modelo do recurso) com a função Edit.

Organizando sistemas gerenciados

À medida que você organiza e categoriza cada sistema:

- Os grupos podem ser aplicados apenas a sistemas DD.
- As propriedades podem ser aplicadas a sistemas, MTrees e contextos de replicação.
- Um conjunto padrão de propriedades do sistema (modelo do sistema, versão do DDOS e nome do domínio) é atribuído automaticamente quando um sistema é adicionado. As propriedades Custom podem ser configuradas. As propriedades do datacenter também podem ser modificadas, mas não excluídas.

Depois de concluir a configuração inicial para cada sistema, você pode atribuir valores a propriedades ou colocar um sistema em um grupo selecionando um sistema e clicando em **Edit**.

Criando grupos

Os grupos são maneiras de organizar os sistemas Data Domain ou PowerProtect com um nome específico, em uma estrutura hierárquica criada pelo administrador do DDMC.

Sobre esta tarefa

Os grupos são úteis para a realização de pesquisas. Quando usados com filtros, os grupos reduzem o número de sistemas retornados. Os grupos podem conter outros grupos e sistemas. Um grupo pode pertencer a apenas um grupo, mas um sistema pode pertencer a muitos grupos. Comece criando um ou mais grupos raiz no nível Grupos e, em seguida, adicione subgrupos e sistemas.

NOTA: Sistemas podem ser adicionados ao nó de Grupos raiz. No entanto, as estruturas de hierarquia de grupo não podem ser alteradas. Elas devem ser excluídas e criadas novamente para alterar a estrutura.

Etapas

1. Selecione **Administration** > **Groups**.
2. Para adicionar um grupo no nível de raiz, clique em **+ ADD**.
3. Certifique-se de que apenas "/" esteja na caixa de caminho. Digite um nome para o novo grupo e clique em **SAVE**.
   O grupo novo é listado no painel Groups.
4. Para adicionar um subgrupo a um grupo, selecione um grupo (que será o grupo *pai*) no painel Groups, clique em **+ ADD** (sinal de mais verde), digite um nome para o subgrupo e clique em **SAVE**.
   O subgrupo é armazenado sob o grupo pai no painel Groups.

5. Depois que um sistema tiver sido adicionado ao DDMC, ele poderá ser adicionado a um grupo. Selecione o grupo de destino no painel Groups e clique em ADD (sinal de mais verde). Na caixa de diálogo **Add Group**, selecione um sistema no painel **Available Systems**, selecione **>** para mover o sistema para Systems no painel Group e clique em **SAVE**.
O sistema é exibido no painel Group Details quando o grupo é selecionado no painel Groups. Quando um sistema reside em mais de um grupo, você pode posicionar o cursor sobre o controle de informações para exibir as atribuições do grupo.

Gerenciando grupos

Embora a modificação e a criação de grupos possam ser realizadas somente pelo administrador do sistema do DDMC, qualquer usuário pode aplicar designações de grupo a seus sistemas Data Domain ou PowerProtect e pode ver a estrutura completa do grupo, embora as permissões do RBAC controlem os sistemas que são exibidos para cada usuário.

Todas as permissões que são aplicadas a um grupo afetam todos os sistemas nesse grupo. Uma imagem de bloqueio é adicionada ao ícone de pasta grupos quando as permissões forem aplicadas diretamente a esse grupo.

Use a página **Administration** > **Groups** para fazer o gerenciamento de grupo:

- Use **ADD** para criar grupos ou para adicionar sistemas a grupos existentes.
- Use **DELETE** para remover sistemas da organização do nível de grupo. (Não é possível usar a opção excluir para remover os sistemas de um grupo. Mas você pode editar o grupo e remover sistemas selecionando-os no painel direito e selecionando a seta para a esquerda.)
- Use **EDIT** em um grupo selecionado para modificar a presença de sistemas dentro desse grupo ou o nome do grupo.
  NOTA: Os grupos não podem ser arrastados e soltos em um local diferente; eles devem ser alterados com a função **Edit**.

Números de porta e nomes do host do proxy de entrada e de saída usados pelo firewall

Os nomes do host (ou endereços IP) de proxy de entrada e saída e números da porta de um firewall deverão ser definidos se a conexão entre o DDMC e o sistema Data Domain ou PowerProtect for feita por meio de um proxy.

NOTA: Esta seção é desabilitada ao adicionar sistemas de alta disponibilidade.

NOTA: No DDMC, as portas 8009 e 8080 são restritas apenas ao localhost e não podem ser acessadas de fora. O DDMC é acessado pela porta 80 HTTP padrão ou, se o SSL estiver habilitado, pela porta 443 HTTPS padrão.

Os termos *entrada* e *saída* são desde a perspectiva do DDMC. *Entrada* significa do sistema para o DDMC e *saída* significa do DDMC para o sistema.

Iniciando a explicação com a situação mais simples (conexão direta), aqui constam alguns cenários e como você pode configurar os nomes do host do firewall do proxy de entrada e saída (ou endereços IP) e números da porta.

DDMC se conectando diretamente a um sistema DD (caso simples)

No caso mais simples de conexão do DDMC com um sistema Data Domain ou PowerProtect, o sistema consegue resolver "ddmc.myco.com" para 1.1.1.1 e o DDMC consegue resolver "ddr.myco.com" para 1.1.1.2.

Figura 3. Caso simples: DDMC conectando-se diretamente a um sistema

Neste caso mais simples, presume-se que:

- O DDMC consegue se conectar ao sistema usando TCP.
- O sistema é igualmente capaz de se conectar ao DDMC usando o TCP.
- O DDMC, por padrão, tenta converter o nome do host de um sistema (ou seja, o nome que será retornado usando `net show hostname` ou o nome que você visualiza no DD System Manager) para um endereço IP que utilize DNS ou um arquivo de host.

- De mesma forma, o sistema tenta converter o nome do host do DDMC para um endereço IP usando DNS ou um arquivo de host.
- O DDMC conecta-se à porta TCP 3009 no sistema e o sistema conecta-se à porta TCP 3009 no DDMC.

Um sistema com várias interfaces de rede

Quando um sistema tiver diversas interfaces de rede, será preciso controlar a interface específica usada pelo DDMC.

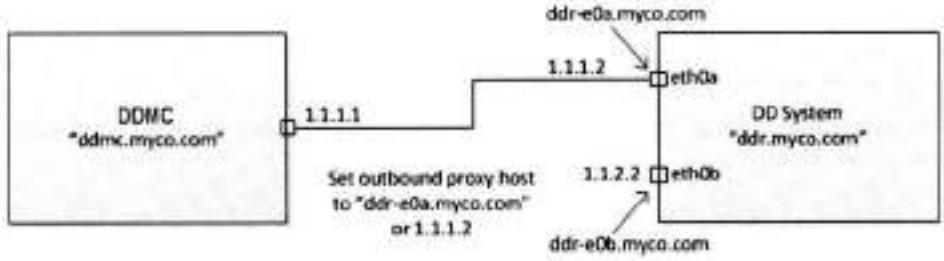


Figura 4. Sistema com várias interfaces de rede

Nesse caso, o nome do host do sistema provavelmente não converte no endereço IP da interface de rede desejada. Para direcionar o DDMC para a interface desejada, você deve definir o nome do host do proxy de saída (ou endereço IP) para um nome de DNS ou o endereço IP da interface desejada. Não é necessário definir o nome do host ou número da porta do proxy de entrada.

Firewall NAT entre o DDMC e sistema

Quando houver um firewall NAT (network address translation) entre o DDMC e um sistema Data Domain, o firewall será configurado para que, ao se conectar a uma porta no firewall, o firewall faça o proxy dessa conexão para um endereço IP e número da porta no sistema de destino. O endereço IP ao qual o DDMC se conecta não corresponde a nenhum endereço IP no sistema em si. Os números da porta também podem ser mapeados novamente. Para se conectar a um sistema, você deve se conectar a uma porta diferente da 3009 no proxy.

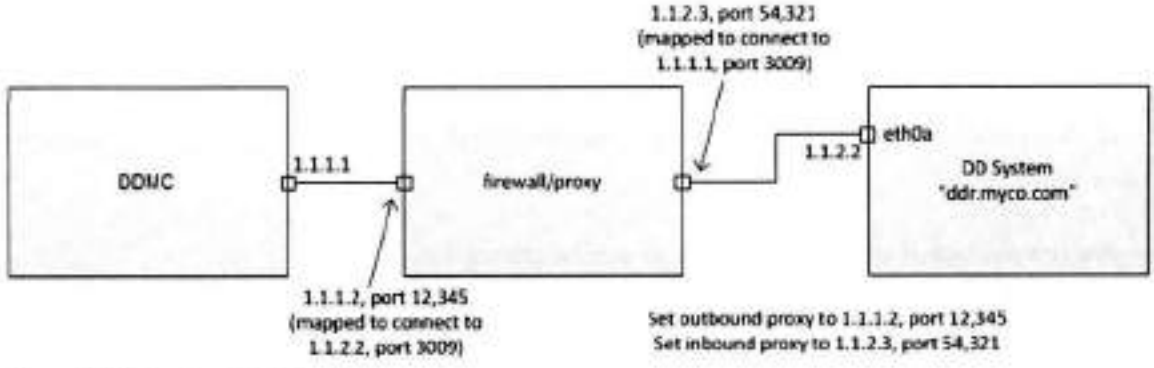


Figura 5. Firewall NAT entre o DDMC e sistema

Nesse caso, quando o DDMC deseja se conectar à porta 3009 no sistema, o DDMC deve tentar se conectar à porta 12.345 no firewall. Por outro lado, quando o sistema Data Domain quiser se conectar à porta 3009 no DDMC, o sistema Data Domain deverá tentar se conectar à porta 54.321 no outro lado do firewall.

Para configurar isso, defina o nome do host do proxy de saída para 1.1.1.2 e o número da porta do proxy de saída para 12.345. Defina o nome do host do proxy de entrada como 1.1.2.3 e o número da porta do proxy de entrada para 54.321. A regra é que o nome do host e o número da porta de saída sejam os endereços aos quais o DDMC deve tentar se conectar quando desejar uma conexão à porta 3009 no sistema Data Domain. O nome do host e número da porta do proxy de entrada são os endereços aos quais o sistema Data Domain deve se conectar quando quiser uma conexão à porta 3009 no DDMC.

Evitando a adição de nomes do host ao servidor DNS ou ao arquivo /etc/hosts do peer

Pode haver situações em que você não deseja adicionar o nome do host do DDMC ou o nome do host do sistema, ou ambos, ao servidor DNS de seu peer ou ao arquivo /etc/hosts de seu peer.

Nessas situações, dependendo do(s) nome(s) do host que você não deseja adicionar, você pode especificar o endereço IP do DDMC no campo do nome do host do proxy de entrada e/ou o endereço IP do sistema no campo do nome do host do proxy de saída.

Datacenter

Crie, gerencie e monitore a integridade e os alertas de grupos de sistemas no nível do data center.

Uma visão geral é fornecida na página principal do data center e mostra:

- O número de data centers criados
- Quantos sistemas estão e quantos não estão em um data center gerenciado

Antes que você possa gerenciar sistemas em um data center, eles devem ser adicionados primeiro (registre-se). Consulte a seção Adicionar (registrar) sistemas ao DDMC.

Crie um datacenter

Crie um data center para conter seus sistemas.

1. Selecione **Inventory** > **Data Centers**.
2. Clique em **Create**.
3. Defina o data center digitando um nome e uma descrição opcional e clique em **Avançar**.
4. Selecione e adicione sistemas disponíveis ao data center.
5. Analise a página de resumo e faça as edições necessárias. Clique em **Next**.

Exclua um datacenter

1. Selecione **Inventory** > **Data Centers**.
2. Clique em **Delete** no data center a ser excluído.
3. Confirme clicando em **Delete**.

Como visualizar detalhes do data center

Clique na seta no canto inferior direito do cartão do data center criado para expandir os detalhes e ver um resumo do data center.

- Resumo geral do data center
- Capacidade do sistema

Clique na guia **Systems** para analisar informações, adicionar ou remover sistemas do data center.

Clique na seta no canto inferior direito do cartão do data center para minimizar a exibição de detalhes.

Exibindo informações de propriedade

Os valores de propriedade atribuída podem ser exibidos selecionando um elemento (como um sistema Data Domain ou PowerProtect) e exibindo todas as propriedades atribuídas a ele ou selecionando uma propriedade e exibindo todos os elementos aos quais ela está atribuída.

Tarefas relacionadas

Adicionando propriedades a sistemas e pares de replicação na página 28

Exibindo propriedades de um elemento

A maneira como você exibe propriedades de um elemento depende do tipo de elemento: sistemas ou pares de replicação.

Etapas

- **Systems** — selecione **Infrastructure** > **Systems** e selecione um sistema DD.
  Todas as propriedades atribuídas a esse sistema são exibidas no painel Properties.

  NOTA: Também é possível exibir as propriedades selecionando o controle da "engrenagem" no banner dos sistemas. Ao selecionar uma ou mais propriedades na lista de propriedades configuradas, uma coluna para essa propriedade é adicionada à tabela. Para ocultar a propriedade, desmarque a seleção da propriedade na lista. Algumas propriedades não podem ser removidas da tabela, por isso elas não aparecerão na lista de propriedades configuradas no controle da engrenagem.
- **Replication** — selecione **Replication** > **Automatic**, selecione um par de replicação e depois **Pair Details**.
  Qualquer propriedade atribuída ao par de replicação é exibida no painel Properties.

Tarefas relacionadas

Localizando elementos por valor de propriedade na página 39
Adicionando propriedades a sistemas e pares de replicação na página 28

Localizando elementos por valor de propriedade

Você também pode encontrar elementos observando todos os valores de propriedade atribuída.

Etapas

1. Selecione **Administration** > **Properties** e escolha o tipo de propriedade (**SYSTEM** ou **REPLICATION**).
   A tabela mostra todas as propriedades que foram criadas. A seleção de uma propriedade exibe seus valores atribuídos no painel à direita.
2. Para exibir onde a propriedade está atribuída, selecione uma propriedade e, em seguida, o ícone do lado direito da coluna Key.

   Na caixa de diálogo Property Assignment, é possível ver o tipo de propriedade, o elemento onde ela está atribuída e os valores da propriedade.

Tarefas relacionadas

Exibindo propriedades de um elemento na página 38
Adicionando propriedades a sistemas e pares de replicação na página 28

Gerenciando políticas de limite de intervalo de replicação

As *Políticas de limite de intervalo de replicação* avisam quando pares de replicação não concluem a replicação dentro de um determinado intervalo de tempo.

Sobre esta tarefa

Ao atribuir uma política de limite de intervalo de replicação, você tem a garantia de que as notificações serão exibidas na página **Replication** > **Automatic** e no recurso **Replication Lag Status** quando a replicação não for concluída dentro dos períodos de tempo que você definiu para os níveis Warning e Critical.

O padrão da política para o nível de Advertência é de 24 horas, e para o Crítico é de 48 horas.

As políticas de limite de intervalo de replicação podem ser criadas somente para MTree, coleta e replicação de diretório. Políticas de limite de intervalo para replicações sob demanda não são compatíveis.

Etapas

1. Selecione **Replication** > **Automatic**.
2. Selecione um ou mais pares de replicação na tabela.
3. Para criar uma política, selecione **LAG THRESHOLD POLICY** (ou clique com o botão direito no par e selecione a opção).
   a. Na caixa de diálogo **Assign Lag Threshold Policy**, no menu Threshold Policy, selecione **Create a new policy**.
   b. Na caixa de diálogo **Manage Lag Threshold Policies**, selecione **ADD**.

c. Na caixa de texto, digite o nome da política e use os controles slider para definir os pontos de limite dos níveis de intervalo Advertência e Crítico.
d. Clique em **SAVE**.

4. Novamente na caixa de diálogo Lag Threshold Policy, selecione uma política no menu Threshold Policy e clique em **ASSIGN**.

Resultados

A política é aplicada às replicações selecionadas. O nome da política atribuída é exibido na tabela, na coluna Threshold Policy.

Para modificar ou destruir uma política, selecione **Manage Lag Threshold Policies** (ou clique com o botão direito no par e selecione a opção). Na caixa de diálogo Manage Lag Threshold Policies, selecione uma política na lista e selecione **Edit** ou **Delete**. Se uma política excluída tiver sido atribuída em qualquer lugar, ela será substituída pela política Padrão. Selecione **Save** para sair.

NOTA: A política Default não poderá ser renomeada ou excluída, mas poderá ser modificada.

Trabalhando com filtros

Os filtros são usados para definir seletivamente o resultado de uma função do DDMC. Por exemplo, os filtros podem ser usados para definir o escopo de elementos que são exibidos em uma página, personalizar o resultado de um relatório ou definir os sistemas Data Domain ou PowerProtect a serem monitorados por recursos do painel de controle. O controle **Filter** (em forma de funil) é exibido nas páginas e caixas de diálogo sempre que um filtro puder ser usado.

Sobre esta tarefa

O menu drop-down no controle **Filter** permite que você selecione os grupos, as propriedades, os sistemas ou as regras a serem usados para filtragem. Quando um filtro estiver ativo em uma página, o controle **Filter** é selecionado. A filtragem pode ser ativada ou desativada usando o controle **Filter** como uma alternância.

A opção **Filter by rule** possibilita que você crie regras personalizadas que podem ser salvas para serem usadas novamente ou executadas no local atual. A regra pode ser criada usando qualquer um dos critérios de filtro padrão (grupos, propriedades e sistemas), juntamente com quaisquer propriedades ou grupos existentes que foram criados. Controles lógicos (é, não é, contém, não contém etc.) são fornecidos, e as afirmações podem ser completas ou seletivas.

NOTA: O filtro global só está disponível no **Classic view** e não é compatível com suporte na guia **Cloud**.

Para criar uma regra de filtro personalizada:

Etapas

1. No menu drop-down **Filter**, selecione **Filter by rule**.
2. Na caixa de diálogo Filter by Rule, informe um nome para o filtro.
3. Usando os menus de seleção na área **Match the following**, crie os critérios para sua regra. Os critérios consistem em uma ou mais declarações.

   Crie a primeira declaração selecionando um objeto no primeiro menu (System, Group, Model, OS, Domain Name, etc.) e uma condição lógica (contains, does not contain, is, is not etc.), em seguida, o destino (insira o texto de entrada ou uma seleção de menu, com base nas seleções anteriores). Por exemplo, uma declaração pode ser "O modelo é DD880".
4. Se necessário, adicione mais declarações com o controle **Add row** (+) ou adicione condições à regra usando o controle **Block** (...), que adiciona a opção **All** ou **Any** à área Match the following e cria declarações adicionais.
5. Selecione o controle **Save** (disco) para disponibilizar esse filtro na lista do menu **Filter** ou selecione **Filter** para executar o filtro uma vez e sair.
6. Para remover o filtro e retornar ao conteúdo não filtrado, selecione **Clear filter** no menu **Filter**.

   NOTA: O filtro pode ainda estar disponível na opção **Recent filters** na lista de controle **Filter**.

Conceitos relacionados

Visualizando os elementos da página do DDMC na página 29
Ícones e controles globais na página 130
Controles de Painel de Controle na página 132

Tarefas relacionadas

Acessando uma página do DDMC na página 31

4

Monitorar sistemas

Tópicos:

- Como o DDMC ajuda no monitoramento de sistemas DD
- Política de retenção de dados do DDMC
- Algoritmo de projeção de espaço para o DDMC
- Realizando o monitoramento diário
- Monitorando a capacidade
- Verificando a lightbox de detalhes do sistema
- Monitorando a replicação
- Monitorando o status com relatórios

Como o DDMC ajuda no monitoramento de sistemas DD

As ferramentas de monitoramento do DDMC permitem que você examine uma ampla variedade de informações operacionais sobre sistemas gerenciados.

Depois que um sistema DD é adicionado ao DDMC, todas as informações históricas desse sistema são copiadas para o DDMC.

Quando os dados operacionais forem alterados em um sistema, o sistema notifica o DDMC, que consulta imediatamente o sistema para obter os dados operacionais mais recentes.

As ferramentas de monitoramento do DDMC utilizam esses dados para a geração de relatórios históricos e atuais e para a criação de projeções de tendência.

As ferramentas de monitoramento do DDMC são altamente visuais, usando tabelas, gráficos e codificação por cores para ajudá-lo a interpretar os pontos de dados essenciais e notar facilmente os alertas de indicadores críticos.

As ferramentas de monitoramento do DDMC ajudam a focar as áreas de interesse. Elas podem mostrar as verificações avançadas de status de todos os sistemas gerenciados e verificar um grupo específico de sistemas, bem como aprofundar-se para verificar a integridade ou histórico operacional dos componentes de um sistema único. Para realizar o monitoramento da capacidade, você pode verificar facilmente os dados da operação atual e do histórico e executar as previsões de capacidade com base nas tendências de uso.

Com o uso da filtragem e agrupamento de opções fornecidas nas páginas de monitoramento, o DDMC permite que você molde facilmente sua apresentação de dados para poder se concentrar apenas na visualização das informações de que você precisa.

Além dos dados fornecidos na interface, você pode gerar relatórios para compilar os dados operacionais que podem ser exportados. Os relatórios podem ser gerados ad-hoc ou agendados e enviados por e-mail para uma lista de partes interessadas.

Política de retenção de dados do DDMC

O DDMC mantém até dez anos de medidas de capacidade e desempenho dos sistemas DD que ele esteja monitorando. Os dados dos sistemas são consolidados em pontos de amostra de hora em hora, geralmente coletados após 30 minutos. As amostras por hora são consolidadas em amostras diárias, em que a operação de um dia é o equivalente *do meio-dia ao meio-dia*. As amostras diárias são então consolidadas em amostras semanais, com a semana iniciando no domingo.

Para reduzir a quantidade de espaço necessário para armazenar esses dados históricos, o DDMC descarta as amostras mais antigas periodicamente. A quantidade de amostras mantidas depende da natureza dos dados e se a amostra é de dados por hora, por dia ou por semana. A tabela a seguir mostra o período pelo qual o DDMC mantém cada amostra.

Tabela 9. Política de retenção de dados do DDMC

tipo de dados	manter amostras por hora por	manter amostras por dia por	manter amostras por semana por
Utilização do espaço de coleta	3 meses	1 ano	10 anos
Espaço usado de MTree	1 mês	3 meses	10 anos

Tabela 9. Política de retenção de dados do DDMC (continuação)

tipo de dados	manter amostras por hora por	manter amostras por dia por	manter amostras por semana por
Replicação automática (bytes transferidos e intervalo)	1 mês	3 meses	10 anos
Replicação sob demanda (quantidade de arquivos e bytes transferidos)	3 meses	1 ano	10 anos
Desempenho (CPU e rede)	1 mês	1 ano	nenhuma criada ou mantida

Por fim, o DDMC mantém até 2.000 alertas históricos de cada sistema DD que estiver sendo monitorado.

Algoritmo de projeção de espaço para o DDMC

O DDMC utiliza um algoritmo sofisticado para projetar o crescimento na utilização de espaço e para prever quando um sistema DD ficará sem espaço. Esse algoritmo foi desenvolvido e verificado com o uso de anos de relatórios do autosupport e deve ser preciso.

Para esse algoritmo, o DDMC utiliza uma *média de movimento de 7 dias* em vez de valores reais medidos. Isso facilita os efeitos de limpeza do file system e outras atividades que se repetem toda semana (por exemplo, excluir um backup completo antigo e criar um fim de semana inteiro).

O objetivo desse algoritmo é computar uma projeção linear do crescimento do espaço usando um conjunto ideal de pontos de dados recentes. O histórico de dados é analisado para encontrar a projeção com o melhor ajuste, ou seja, a regressão com o mais alto valor R^2.

O valor R^2 é uma medida de quão próximo a regressão ajusta as medições reais. Um valor "1" significa que o ajuste ficou perfeito. Um valor "0" significa que não houve nenhum ajuste. Um valor "0,8" significa que o DDMC encontrou uma projeção que corresponde às medições quase que o suficiente para ser significativa e não equivocada.

Depois que o melhor ajuste for determinado, a projeção deve passar nos seguintes testes de validação para garantir que a previsão seja precisa:

1. O DDMC deve ter pelo menos 15 dias de dados históricos.
2. O valor R^2 da regressão deve ser de pelo menos 0,8 ou superior.
3. O tempo futuro para completar deve ser menor que 10 anos.
4. O sistema deve estar pelo menos 10% completo.
5. A amostra de dados mais recente deve estar dentro de 5% da projeção.

A combinação de todos esses de critérios de validação é responsável pelo comportamento típico de uso de sistema, como o espaço que fica livre após um ciclo de limpeza, dá um salto na utilização à medida que novas cargas de backup são armazenadas no sistema, e o espaço vai ficando livre quando os backups são excluídos.

Realizando o monitoramento diário

O uso do DDMC para realizar o monitoramento diário de seu site permite que você verifique uma atividade incomum antes que ela se torne um problema sério.

Você deve executar as seguintes tarefas *pelo menos diariamente* para obter uma visão geral do status operacional da replicação de dados e de seus sistemas Data Domain ou PowerProtect.

Verificando recursos de status do painel de controle

Os widgets **Home** > **Dashboard** (Health Status, Active Alerts, Capacity Thresholds, Capacity Used, Replication Status, Lag Thresholds, High Availability Readiness e Cloud Health) fornecem uma visão geral dos principais indicadores de desempenho para seus sistemas Data Domain ou PowerProtect monitorados.

Por padrão, é fornecida uma guia chamada **All Systems** que é preenchida com um recurso de cada tipo.

Os gráficos, dials e alertas com codificação por cores facilitam detectar problemas do sistema operacional. Muitos componentes nos recursos fornecem um link para uma página com recursos completos para a função, a fim de que você possa aprofundar-se e consultar informações completas.

Se qualquer um dos sistemas monitorados não estiver acessível (porque está off-line, não responde, a versão do SO é incompatível, não está transmitindo ou é não gerenciado), um botão **Status** é exibido no canto superior direito de um recurso (exceto para Active Alerts). A seleção deste botão mostrará a contagem de sistemas com problemas de conexão. A seleção do link **Show Health Status** abrirá a página **Health** > **Status**, onde é exibida uma lista desses sistemas.

Modelos de recurso para funções de monitoramento usadas com frequência podem ser usados para criar recursos para todos os sistemas gerenciados ou filtrados por um conjunto de critérios, como grupos, propriedades, sistemas ou regras.

Depois de criados, você pode arrastar os recursos em todo o painel de controle para melhorar sua organização. Um recurso ou uma guia com vários recursos pode ser copiada e modificada para criar recursos adicionais.

O tamanho do painel de controle pode ser alternado entre o modo de exibição normal e de tela cheia.

Verificando a capacidade do sistema

Os recursos de capacidade do sistema o ajudam a detectar deficiências na capacidade geral de armazenamento gerenciado e a monitorar a utilização de armazenamento do sistema gerenciado.

Capacity Thresholds

O recurso Capacity Thresholds exibe os sistemas que ultrapassaram os níveis de advertência ou crítico de capacidade de armazenamento.

Capacity Used

O recurso Capacity Used permite que você monitore totais agregados de níveis de armazenamento para todos os sistemas DD que estiverem configurados para gerenciar. Esse recurso monitora a capacidade de armazenamento total de todos os sistemas (para o espaço que é utilizado e que está disponível) ou um grupo selecionado, se um filtro for definido.

Verificando o progresso de replicação

Os recursos de replicação informam status de replicação e problemas.

Status da replicação

O recurso Replication Status destaca as replicações com problemas de desempenho para os sistemas monitorados do recurso.

Lag Thresholds

O recurso Lag Thresholds identifica pares de replicação que não estão replicando dados para o destino com a rapidez suficiente e mostra a contagem de pares de replicação que ultrapassaram os níveis de limite Critical, Warning e Normal, com base nas políticas atribuídas. Este recurso identifica os pares, a duração do tempo de atraso e se há melhora.

Verificando a integridade e alertas

Os recursos Status e alertas de integridade do painel de controle destacam os sistemas que estão reportando maior acessibilidade ou problemas operacionais. E, se houver problemas, os recursos fornecem links de aprofundamento para detalhes do sistema.

Status de integridade

O recurso Health Status destaca sistemas inacessíveis e que estejam enfrentando problemas com o file system e operação de replicação, alertas e protocolos de transmissão de dados. Os recursos mostram All Normal (verde) ou mostram uma contagem de sistemas que apresentam problemas.

Ao clicar no indicador, você navega para a página **Health Status**, filtrada pelos sistemas no status Not Healthy, se houver.

Health Status

O recurso Active Alerts exibe um registro de sistemas com alertas pendentes Emergency & Alert, Critical & Error, e Warning, usando indicadores coloridos e uma contagem total de Alertas de cada sistema. O pior status terá prioridade.

Clique no indicador para ir à página Alerts, filtrada pelos filtros configurados no recurso.

Verificando notificações de alerta

Para alertas novos e não confirmados nos sistemas que você está autorizado a gerenciar, sempre verifique o ícone de campainha que aparece no lado superior direito.

Essa área de notificação não é limitada pelas configurações de filtro ativas, ou seja, exibe as notificações de alertas para todos os sistemas que você está autorizado a gerenciar.

A área "New Alerts" mostra os alertas atuais e não confirmados de nível Emergency, Error e Warning. Clique em qualquer lugar na área New Alerts para exibir um pop-up com a geração de relatórios de severidade, o nome do sistema e a classe do novo alerta. Após a exibição do pop-up, a notificação de alertas é removida da área de notificações de alertas.

Para consultar os detalhes do alerta, selecione o link "Show me these alerts" para abrir a página **Health** > **Alerts**, na qual a tabela é filtrada para mostrar somente os novos alertas.

Verificando o status de integridade

A página **Health** > **Status** exibe informações sobre possíveis problemas operacionais, como o status de conexão, status de replicação e alertas.

Os ícones Systems/Groups/Tenants no canto superior direito permitem mostrar todos os sistemas Data Domain e PowerProtect organizados por grupo ou por atribuição de tenant.

As cores de LED indicam:

- Vermelho — erro ou problema
- Amarelo — erro ou advertência
- Verde — operação normal
- Cinza — componentes desabilitados
- Cinza "Empty Socket" — componentes não licenciados

NOTA: Se um sistema estiver inacessível, mas não desabilitado ou não licenciado, o último estado conhecido do LED é exibido. Um sistema inacessível ou sem transmissão ainda pode estar operacional para backups, restauração e replicação, mas não estar se comunicando com o DDMC.

Para as três visualizações:

- Passe o cursor sobre um LED cinza na coluna Replication para obter um link para a Replication Overview que mostre os pares relacionados a esse sistema ou unidade de tenant.
- Passe o cursor sobre um LED vermelho/amarelo na coluna Alerts para obter um link para abrir a página Alerts.
- Use a opção Sort Ascending para a coluna Connection Status para localizar problemas de conexão em sistemas.
- Se o file system for destruído ou desabilitado, um LED vermelho será exibido. Como resultado dessa não atividade, Protocols e Replication são afetados e também exibem um LED vermelho.

Para as exibições de Systems ou Groups:

- Passe o cursor sobre um LED de "soquete vazio" para obter um link para visualizar o DD System Manager.
- O controle System Details (canto superior esquerdo) inicia a Lightbox System Details para o sistema selecionado.

Para exibição de tenants:

- Quando um sistema estiver off-line, as unidades de tenant nesse sistema também ficam off-line, e o ícone off-line da unidade de tenant é exibido na árvore da unidade de tenant.
- Não são exibidas as unidades de tenant não gerenciadas, os MTrees e as unidades de armazenamento que não pertencem a uma unidade de tenant.
- São exibidos somente tenants e unidades de tenant que pertencem ao usuário atual.
- O controle Tenant Unit Details (canto superior esquerdo) inicia o Tenant Unit Details Lightbox para a unidade de tenant selecionada.

Verificando alertas de integridade

Além de verificar o status de integridade para problemas operacionais, verifique também a página **Health** > **Alerts**. Fique atento a alertas novos e repetidos.

Use os ícones de sistemas/tenants no canto superior direito da página para alternar o conteúdo da página e exibir todos os sistemas Data Domain e PowerProtect ou sistemas organizados por atribuição de tenant.

Ao selecionar o ícone de tenants, observe o seguinte:

- O controle Tenant Unit Details (canto superior esquerdo) inicia a lightbox de Tenant Unit Details.
- Um alerta especial para "todas" as unidades de tenant é aplicado a todas as unidades de tenant no sistema.

O banner da página fornece resumos do número total de alertas: os que são erros e acima, e os que são advertências.

No canto superior direito, você pode selecionar a guia Active Alerts ou All Alerts. Muitos, mas nem todos, os alertas permanecem ativos até serem removidos manualmente.

Os filtros de intervalo de data (últimas 12 horas, últimas 24 horas, últimos 7 dias, últimos 30 dias, todos os alertas ativos e personalizado) permitem reduzir ou expandir o foco do alerta em escopo ou voltar a um ponto específico no tempo.

Os controles da coluna classificam a lista de alertas por Severity, System Name, Post Time, Class, Message e Object ID. A coluna System Name inclui um filtro para a inserção do texto com o nome do sistema.

A seleção de um alerta na tabela se expande para mostrar informações descritivas sobre o alerta. Para ver um resumo do histórico do alerta, selecione o link **More details** para ver uma lista de todas as ocorrências do alerta no local.

Para investigar ou resolver um alerta em um sistema, abra o DD System Manager clicando duas vezes sobre o alerta na tabela ou use o controle **View DD System Manager**, que é ativado quando um alerta do sistema estiver selecionado.

NOTA: Para obter mais informações sobre alertas específicos, consulte o Catálogo de mensagem de erro no site de suporte on-line.

Verificando trabalhos de integridade

Além de verificar o Status de integridade para problemas operacionais, verifique também a página **Health** > **Jobs**. Essa página exibe informações sobre os trabalhos (também chamados de tarefas) que foram iniciados no DDMC, inclusive os trabalhos ainda em andamento e os que foram concluídos com sucesso ou não. Detalhes de uma tarefa, inclusive o status de sua subtarefa, são mostrados para uma tarefa selecionada no painel Details.

Você pode filtrar os trabalhos pelo status Failed, In progress e/ou Completed.

Você pode selecionar um trabalho na lista principal e expandir as etapas para consultar até 10 níveis de subetapas.

As tarefas podem ser executadas somente no DDMC ou podem ser executadas no DDMC e em um sistema Data Domain e PowerProtect. Por exemplo, a tarefa Report Generation é executada exclusivamente no DDMC. Outras tarefas, como Update, são executadas principalmente no sistema, mas um processo esqueleto no DDMC acompanha o progresso da tarefa. E ainda outras tarefas são executadas principalmente no DDMC (como Adding Systems), mas têm subtarefas que são executadas no sistema. As tarefas que são executadas no DD System Manager não são exibidas na lista Jobs, apenas as tarefas iniciadas no DDMC são mostradas.

A lista de tarefas exibida depende da função:

- Uma pessoa com uma função *user* ou *limited-admin* em um sistema ou no DDMC vê somente as tarefas que iniciou nesse sistema ou DDMC.
- Um *admin* em um sistema ou DDMC vê todos os trabalhos desse sistema e do DDMC.

Monitorando a capacidade

As páginas Capacity exibem informações sobre a utilização do armazenamento. É daqui que você pode monitorar o consumo de espaço atual e histórico, bem como estimar necessidades de armazenamento futuras projetadas para curto prazo.

A seção **Capacity** está dividida no seguinte:

- Sistemas, que incluem informações de capacidade e informações de projeção
- Nuvem
- MTree

Verificando a capacidade do sistema e a utilização de espaço no disco

A seção **Capacity** exibe os volumes de utilização de armazenamento de sistemas DD monitorados, nuvem e MTrees.

NOTA: Este guia presume que você esteja familiarizado com os termos de capacidade, conforme apresentado no *Guia de Administração do DDOS*. Consulte esse guia ou a ajuda on-line do DD System Manager para obter explicações sobre esses termos.

O sistema, a nuvem e os links de MTree em **Capacidade** no painel de navegação no lado esquerdo da página permitem que você escolha como exibir os dados. A página **Systems** mostra um resumo da capacidade com um banner clicável que também funciona como um filtro. O link **MTree** tem visualizações de alternância para **Sistemas** e **Grupos de usuários**.

A capacidade física (PCM) de MTrees, tenants e unidades de tenant pode ser medida e está descrita em mais detalhes na próxima seção, Measuring Physical Capacity (PCM).

Capacidade dos sistemas

A tabela do limite de capacidade dos sistemas mostra o espaço atual disponível e "% usada e projetada".

- No máximo 25 sistemas podem ser exibidos em uma página
- Três meses é o padrão para a **Linha do tempo de projeção (capacidade utilizada %)**, a data específica pode ser selecionada, mas não pode ser maior que 12 meses
- Deve selecionar uma linha (botão de opção) antes que a opção **Calcular projeções** esteja disponível

Funcionalidade adicional:

- Identificar sistemas como destinos para novos backups, replicação e migração
- Exibir o volume de dados gravados durante um período específico, como um ciclo de backup, e determinar o quanto ele foi compactado
- Identificar os sistemas que se desviaram de seu padrão para a taxa de compactação
- Identificar os sistemas que utilizaram todo seu espaço de armazenamento
- Para sistemas habilitados para Extended Retention, identificar quanto espaço está disponível e utilizado nos níveis Arquivamento e Ativo e como ele está compactado
- Identificar quando a coleta de lixo é executada e a quantidade de espaço que é recuperado
- Classificar as colunas Warning e Critical Capacity Thresholds por controles crescentes/decrescentes e podem ser filtradas por maior, menor ou igual a

Há um painel de detalhes que pode ser deslizado para abrir à direita, usando a seta no canto superior direito da tabela. Quando um sistema é selecionado usando o botão de opção, o painel de detalhes é preenchido com mais informações relacionadas à capacidade.

Para obter informações mais detalhadas, o nome do sistema (na tabela ou no painel de detalhes) pode ser clicado para abrir o Lightbox System Details.

NOTA: Os valores de utilização de espaço podem não corresponder exatamente aos totais de capacidade relatados pelo DD System Manager. Devido a um atraso de consulta de até uma hora, a geração de relatórios do DDMC sempre atrasará. Isto é especialmente verdadeiro se houver muita rotatividade no sistema monitorado. A discrepância estará mais visível e há uma possibilidade de que o DDMC nunca consiga capturar os totais de capacidade do DD System Manager.

Capacidade de nuvem

- Monitorar o nível ativo e a capacidade do nível da nuvem que residem em diferentes provedores de nuvem
- Fornecer uma visão geral da distribuição de dados entre os datacenters no local e os diferentes provedores de nuvem
- Listar os MTrees que estão associados a um determinado fornecedor de nuvem

Capacidade de MTree

- Digitar uma lista de strings separadas por vírgulas para filtrar a coluna Tenant Unit.
- Classificar MTrees dentro de uma unidade de tenant.
- Monitorar a capacidade dos sistemas únicos ou agrupados logicamente para controlar a utilização e identificar os sistemas que estão usando a capacidade muito rapidamente

Na seção **Capacity Usage**:

- Quando uma unidade de tenant é selecionada, as informações são agregadas com base em todos os MTrees dentro desta unidade de tenant.
- Quando um tenant é selecionado, as informações são agregadas com base em todos os MTrees em todas as unidades de tenant relativas a este tenant.
- A última linha mostra os totais agregados.

Na seção **Measured Physical Capacity**, **Job State** pode ter um dos cinco valores a seguir:

- Unsupported (o sistema DD não dá suporte a recursos de PCM)
- Completed (último trabalho bem-sucedido)
- Com falha
- em andamento
- None (é compatível com PCM, mas não há trabalho em execução)

Na área **Charts**, as informações de **Space Usage**, **Consumption** e **Data Written** podem ser visualizadas selecionando cada uma na lista drop-down. Se houver sistemas conectados no Cloud Tier ou no Retention Tier, as guias serão exibidas como Retention (para Cloud Tier e Retention Tier) e Total. Gráficos novos para Cloud Tier também estão disponíveis.

- Sistemas que estão consumindo espaço em um ritmo maior ou menor do que seu padrão histórico
- Capacidade total, quantidade consumida e taxa de compactação (agregada) para um grupo de sistemas
- Taxa de inclusão de dados para um grupo de sistemas, por exemplo, a taxa de inclusão total de dados das últimas 24 horas
- Sistemas que estão sem espaço ou com espaço criticamente baixo, ou que usaram todo o espaço de armazenamento
- O volume de dados que foi feito backup da noite anterior (período de 24 horas) e a taxa de compactação para um grupo de sistemas
- A última vez que a coleta de lixo foi executada e a quantidade de espaço que foi recuperado
- Selecione vários sistemas e veja informações agregadas

Medindo a capacidade física

A *PCM (Physical capacity measurement, Medição da capacidade física)* apresenta informações sobre a utilização de espaço de um subconjunto de espaço de armazenamento para MTrees, unidades de tenant e tenants.

A PCM mede a capacidade física consumida por um subconjunto de arquivos dentro do file system com base em como os arquivos no subconjunto se desduplicam com outros arquivos no subconjunto. Em outras palavras, ela mede a capacidade física que é consumida em um sistema Data Domain ou PowerProtect por um conjunto de arquivos caso esse conjunto de arquivos contenha os únicos arquivos no sistema. Essa é uma medida do tipo *ponto no tempo*, com base em quando a medida é solicitada.

Você pode especificar o subconjunto do file system para medir de várias maneiras: como um MTree, uma unidade de tenant (todos os arquivos dentro de uma unidade de tenant) ou um tenant (todos os arquivos dentro de um tenant). Como um tenant pode estender os sistemas, nesse caso, o DDMC mede e relata a capacidade física consumida pelo tenant em cada sistema.

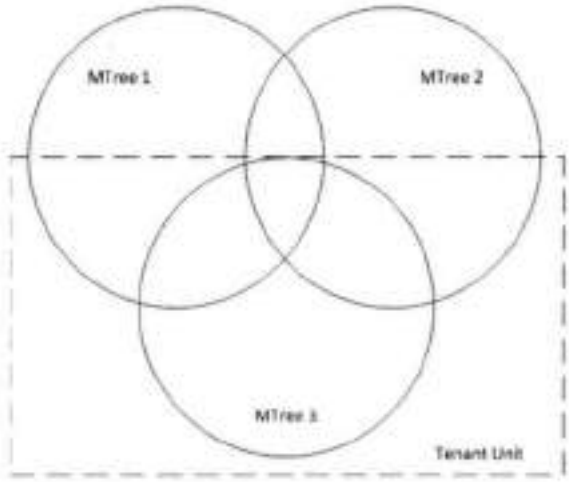
Não mais que um resultado por hora da PCM é mantido no período dos últimos 90 dias; depois essa quantidade passa para não mais que um por dia no período do último ano; e por fim, não mais do que um por semana no período dos últimos 10 anos.

Gerenciando agendamentos de medição de capacidade física

Você pode fazer agendamentos de medição de gerenciamento da capacidade física usando a caixa de diálogo Manage Measurement Schedules.

Sobre esta tarefa

NOTA: Não é possível somar diretamente as Medições de capacidade física porque uma determinada quantidade de *compartilhamento* ocorre entre MTrees, portanto qualquer total gerado normalmente pode ser equivocado. Na figura a seguir, informações da unidade de tenant são armazenadas em três MTrees, mas há compartilhamento entre esses MTrees, por isso o total real é menor do que simplesmente adicionando o espaço utilizado pela unidade de tenant.



Os agendamentos podem ser consolidados em vários sistemas Data Domain e PowerProtect da seguinte maneira:

- Se dois ou mais agendamentos tiverem o mesmo nome, tipo e agendamento (por exemplo, "todas as segundas-feiras, às 7h"), o DDMC exibirá um agendamento configurado em sistemas diferentes.
- Se dois agendamentos tiverem o mesmo nome, mas tipos ou horários agendados diferentes, o DDMC exibirá dois agendamentos.
- Se um agendamento estiver *Disabled* em um sistema, mas *Enabled* em outro, o DDMC exibirá um agendamento.

NOTA: A atualização pode levar até uma hora se essas alterações forem feitas por meio da interface de linha de comando (CLI).

Etapas

1. Selecione **Capacity** > **MTrees** > **Physical Capacity Measurement menu** > **Schedules**

   Na visualização Clássica, selecione **Capacity** > **Utilization** > **MTree tab** > **Physical Capacity Measurement menu** > **Schedules**.
2. Na caixa de diálogo Manage Measurement Schedules, é possível adicionar um novo agendamento, editar um agendamento existente ou excluir um agendamento.
3. Para agendamentos existentes, expanda a seta à esquerda para exibir as entidades que pertencem ao agendamento selecionado:
   - **Schedule** mostra o agendamento atual, como *Daily at 12:00*.
   - **Type** pode ser *MTree*, *unidade de tenant* ou *tenant*.
   - **Status** indica se o agendamento está *Habilitado* ou *Desabilitado*. Se desabilitado, ele não será executado na hora agendada.

     NOTA: Se o agendamento foi habilitado em alguns sistemas e desabilitado em outros, a seleção de *Enable* o habilitará em todos os sistemas. Da mesma forma, a seleção de *Disable* o desabilitará em todos os sistemas.
   - **Em uso** exibe *Sim* se qualquer entidade estiver atribuída a esse agendamento.
4. Selecione **Close** quando tiver terminado.

Adicionando ou editando agendamentos de medição de capacidade física

Você pode adicionar ou editar os agendamentos de medição de capacidade física usando a caixa de diálogo Manage Measurement Schedules.

Sobre esta tarefa

NOTA: Se você alterar o nome de um tenant que faz parte de um agendamento de PCM, a alteração do nome não será atualizada automaticamente no agendamento. Você deve adicionar manualmente o novo nome do tenant ao agendamento de PCM.

Etapas

1. Selecione **Capacity** > **MTrees** > **Physical Capacity Measurement menu** > **Schedules**

   Na visualização Clássica, selecione **Capacity** > **Utilization** > **MTree tab** > **Physical Capacity Measurement menu** > **Schedules**.
2. Na caixa de diálogo Manage Measurement Schedules, selecione Add (sinal de mais verde) ou selecione um agendamento e selecione Edit (lápis amarelo).
3. Na caixa de diálogo Add a Schedule ou Edit schedule, especifique ou edite as seguintes informações:
   - **Status** é exibido apenas para edição. Selecione *Enabled* ou *Disabled*.

- **Name** pode ser inserido apenas para um novo agendamento. Você não pode editar o nome depois que o agendamento tiver sido criado.
- **Every** pode ser *Day*, *Week* ou *Month*. A seleção de Week ou Month criará um calendário semanal ou mensal, no qual você pode selecionar os dias da semana ou os dias do mês.
- **Scope** indica se o agendamento é de *MTree*, de *tenant* ou de *unidade de tenant*. Você não pode criar um agendamento com diferentes tipos de entidades; no entanto, você deve selecionar uma para criar um agendamento. Você não pode editar o escopo depois de criá-lo.
- **Assignment** exibe *Yes* se qualquer entidade for atribuída a esse agendamento.

4. Selecione **Adicionar**.

Excluindo agendamentos de medição de capacidade física

Você pode excluir os agendamentos de medição de capacidade física usando a caixa de diálogo Manage Measurement Schedules.

Etapas

1. Selecione **Capacity** > **MTrees** > **Physical Capacity Measurement menu** > **Schedules**

   Na visualização Clássica, selecione **Capacity** > **Utilization** > **MTree tab** > **Physical Capacity Measurement menu** > **Schedules**.
2. Na caixa de diálogo Manage Measurement Schedules, selecione um agendamento e selecione Delete (X vermelho).
3. Na caixa de diálogo Delete *schedule*, selecione as setas para baixo ao lado de **More information** para ver as entidades atribuídas a esse agendamento.
4. Selecione **Yes** ou **No**.

Atribuindo ou cancelando a atribuição de agendamentos de medição de capacidade física

Você pode atribuir e cancelar a atribuição de agendamentos de medição de capacidade física de MTrees, unidades de tenant ou tenants, usando a caixa de diálogo Assign/Unassign Schedules. A atribuição de um agendamento a um grupo de usuários medirá esse grupo em todos os sistemas DD utilizados pelo grupo de usuários.

Etapas

1. Selecione todos ou vários MTrees, um único MTree, uma unidade de tenant ou um tenant aos quais você deseja atribuir ou cancelar a atribuição de agendamentos.
2. Selecione **Capacity** > **MTrees** > **Physical Capacity Measurement menu** > **Assign/Unassign Schedules**.

   Na visualização Clássica, selecione **Capacity** > **Management** > **MTree tab** > **Physical Capacity Measurement menu** > **Assign/Unassign Schedules**
3. Na caixa de diálogo Assign/Unassign Schedules para *entidade*, você pode mover os agendamentos da lista Available Schedules para a lista Assigned Schedules e vice-versa usando as setas. As setas duplas (>> e <<) movem tudo. As setas simples (> e <) movem apenas o agendamento selecionado.
4. Selecione **Save** ou **Cancel**.

Medir agora a capacidade física

Você pode executar uma tarefa *measure now*, ou seja, uma medida única de capacidade física de MTrees, unidades de tenant ou tenants usando a caixa de diálogo Measure Now.

Etapas

1. Selecione todos ou vários MTrees, um único MTree, uma unidade de tenant ou um tenant que você deseja *medir agora*.
2. Selecione **Capacity** > **MTrees** > **Physical Capacity Measurement menu** > **Measure Now**.

   Na visualização Clássica, selecione **Capacity** > **Management** > **MTree tab** > **Physical Capacity Measurement menu** > **Measure Now**
3. Na caixa de diálogo Measure Now, você pode selecionar **Hide** para manter o processo em andamento, mas não mostrar a caixa de diálogo. É possível monitorar o andamento na página Jobs.
   a. Se o trabalho for concluído com sucesso, a mensagem de sucesso será exibida.

b. Se o trabalho apresentar falha, o motivo da falha será exibido ao passar o cursor do mouse sobre o status "Falha".
c. Para entidades associadas a vários sistemas (um tenant único ou vários MTrees), se ocorrer um erro, será exibida uma tabela com o erro por sistema Data Domain.
d. Depois que o trabalho for iniciado, pode levar algum tempo para que ele seja concluído.

NOTA: Uma medida de capacidade física demora aproximadamente o mesmo tempo que um ciclo de limpeza. Pode levar horas ou, em casos extremos, dias. O tempo depende da carga de trabalho do sistema no momento e da quantidade de dados no MTree, unidade de tenant ou tenant.

Pode levar até uma hora para os dados da medição da capacidade física aparecerem nas páginas do MTree, depois que o trabalho for concluído.

Visualizando trabalhos de medição de capacidade física

Use a caixa de diálogo **View Measurement Jobs** para visualizar os trabalhos de medição de capacidade física, tanto de um MTree, quanto de um tenant ou de uma unidade de tenant.

Sobre esta tarefa

O número de amostras de medição de capacidade física que são apresentadas pelo DDMC é geralmente diferente do número de amostras que são exibidas pelo DDOS. O DDOS limpe as amostras históricas de medição de capacidade física para MTrees, unidades de grupo de usuários e grupos de usuários diariamente e mantém a distribuição das amostras históricas por não mais que uma amostra por hora no período dos últimos 90 dias; depois não mais do que uma por dia no período do último ano; e por fim, não mais do que uma por semana nos últimos 10 anos. O DDMC remove amostras de medição de capacidade física e mantém no máximo 730 dias de dados PCR. Como não possui dados periódicos regulares, eles são removidos como alertas.

Etapas

1. Selecione **Capacity** > **MTrees** > **Physical Capacity Measurement** > **View Measurement Jobs**

   Na visualização Clássica, selecione **Capacity** > **Management** > **MTree tab** > **Physical Capacity Measurement** > **View Measurement Jobs**.
2. Na caixa de diálogo View Measurement Jobs for entity, observe a lista combinada dos trabalhos de medição de capacidade física que estão como In-progress, Completed e Failed, começando pelo mais recente.
3. Selecione **Close**.

Verificando a capacidade projetada do sistema

As informações de projeção estão disponíveis com as informações de capacidade na página **Sistemas de** > **Capacidade** e ajudam a planejar as necessidades de capacidade futuras.

Você pode usar essas informações para:

- Prever quando os sistemas ficarão sem espaço de armazenamento ou atingirão um ponto criticamente baixo.
- Determinar as necessidades futuras de capacidade projetando tendências históricas e atuais.
- Determinar destinos de migração projetando os sistemas que estão ficando cheios, em comparação aos mesmos sistemas de modelo que terão espaço disponível.
- Executar exportação CSV.

Clique em **Calcular projeções** para que o pop-out seja exibido.

- Selecione datas em **Data para o cálculo da projeção**
- O gráfico e o controle deslizante abaixo do gráfico atualizam o intervalo de datas visíveis no gráfico
  - Clicar e arrastar o gráfico seleciona e "amplia" a seção do gráfico.
  - Em seguida, clique no ícone - no canto superior direito nesta exibição ampliada para exibir todos os dados disponíveis.
- Passar o mouse sobre o gráfico exibe as datas e valores no lado direito do gráfico.
- Por outro lado, a seleção da data no lado direito mostra os dados (históricos ou futuras projeções) para essa data.

Capacidade > **Projetaada** da visualização clássica do DDMC

Cada entrada na tabela mostra o nome do sistema e um ícone de status da conexão com uma caixa de diálogo que contém um link para a página **Health** > **Alerts**. Os volumes de utilização de espaço (tamanho, utilizado e livre) dos meses atuais e projetados são fornecidos. Um gráfico de armazenamento representa a capacidade do sistema pela porcentagem usada com codificação por cores para mostrar os

níveis de limite normal, de advertência e crítico. Esse gráfico é uma versão em miniatura do gráfico de projeção padrão na parte inferior da página.

O controle Projected Capacity (By Date) apresenta informações em três grupos de colunas. Há também um gráfico sparkline para apresentar a forma geral da variação.

- 100% Capacity mostra a projeção de quando o sistema estará 100% cheio, com base na taxa de aumento determinada automaticamente.
- Projected Capacity permite computar a capacidade utilizada em uma data específica. O sistema pode ter a capacidade livre, estar cheio ou estar cheio demais. Essas colunas projetam o quanto o sistema estará acima da capacidade para que você saiba quanta capacidade deve liberar ou comprar.
- Current Capacity mostra o estado atual do sistema DD, que é o mesmo da página **Capacity** > **Utilization**.

Mensagens informativas serão exibidas se dados insuficientes impedirem uma projeção precisa.

Tabela 10. Mensagens de dados insuficientes

Mensagem	Descrição
Os dados não estão mais sendo adicionados ao sistema.	A capacidade utilizada é simples, por isso, as previsões não são confiáveis.
A projeção não pode ser realizada.	A projeção falhou por motivos desconhecidos.
A projeção não pode ser realizada, pois o espaço médio utilizado nos últimos 7 dias é menor que 10%.	O sistema tem tão poucos dados que o file system tem utilização menor que 10%. Não é possível fazer uma projeção quando um volume tão reduzido de capacidade é usado porque não é confiável.
A projeção não pode ser feita devido à insuficiência de dados. Um mínimo de 15 pontos diários de utilização de espaço é necessário para projeções.	Pelo menos 15 dias de dados é necessário para fazer uma projeção confiável.
A projeção não pode ser feita, pois a tendência de utilização de espaço não é consistente durante o intervalo de datas especificado.	Uma regressão foi computada e a inclinação é negativa (ou seja, a capacidade está sendo liberada, não consumida) e a data de preenchimento foi no passado.
A projeção não pode ser feita, pois a tendência de utilização de espaço não é consistente durante o intervalo de datas especificado.	• O último ponto de utilização medido está abaixo do intervalo de confiança da projeção. O intervalo de confiança é a faixa de 95%, ou seja, durante 95% do tempo, os pontos de dados reais devem estar dentro do intervalo de confiança. O ponto mais recente medido é inferior ao menor valor esperado com confiança de 95%. • Uma regressão foi computada, mas a melhor regressão não corresponde precisamente às medições reais de perto. Tecnicamente, esse resultado indica que o valor R^2 (o "coeficiente de determinação") é menor que 0,8. [Um valor R^2 1 significa que um ajuste perfeito foi encontrado. Um valor 0 significa que nenhuma correlação foi encontrada.] Esse valor R2 significa que a capacidade não está sendo utilizada de maneira linear e sem interrupções. Ela está sendo consumida em uma taxa variável ou está variando entre o que está sendo utilizado e liberado. (Consulte Algoritmo de projeção de espaço para o DDMC na página 43 para saber mais sobre o R^2.)

Os dados da coluna Date (atuais e os selecionados com o uso do cronograma) podem ser classificados por volume de espaço utilizado, espaço livre, % utilizado e tamanho em ordem crescente ou decrescente.

Destacar um sistema na lista ativa os controles para personalizar a projeção de modo interativo e iniciar o DD System Manager.

Interagindo com o gráfico de projeção

Você pode executar uma projeção personalizada usando o gráfico interativo de projeção na parte inferior da página **Capacity** > **Projected**.

Etapas

1. Para ajustar a faixa visível dos dados mostrados no gráfico (isso não altera as datas projetadas):
   - No controle Date Range, no canto superior esquerdo do gráfico, basta selecionar 1w, 1m, 3m, 1y ou All. Os campos de entrada no canto superior esquerdo alteram a faixa visível de dados e os da direita alteram as datas de projeção.
   - Informe as datas específicas nos campos de entrada de datas.

- Para alterar as projeções, você pode deslizar ou ajustar a área cinza no gráfico. Você pode mover esses controles para a esquerda ou direita, ou pode tornar o gráfico mais largo ou mais estreito para ajustar um intervalo de tempo que você acredita que seja mais representativo que aquele calculado pelo DDMC como o melhor ajuste.

Uma melhor correlação entre a linha de tendência projetada mostrará um intervalo de confiança mais estreito ao redor da linha de tendência projetada. Uma correlação menos satisfatória mostrará um intervalo maior de confiança.

2. Nas datas usadas para realizar o controle de projeções, no canto superior direito do gráfico, as datas serão atualizadas para refletir a projeção personalizada.
3. Use o botão Defaults para retornar às projeções padrão/melhor ajustadas.

Verificando a lightbox de detalhes do sistema

A *lightbox System Details* apresenta informações detalhadas de operação sobre componentes específicos de um sistema Data Domain ou PowerProtect.

Há um controle **System Details** em cada uma das páginas a seguir:

- **Health** > **Status**
- **Sistemas de** > **Capacidade**
- **Mtrees** > **de capacidade**
- **Replication** > **Overview**
- **Sistemas** > **de infraestrutura**

NOTA: Na visualização Clássica:

- **Capacity** > **Utilization**
- **Capacity** > **Projected**

Para ativar o controle, primeiro você deve selecionar um sistema DD na tabela.

Há cinco guias para sistemas que não são de alta disponibilidade e seis para sistemas de alta disponibilidade.

A guia **Overview** mostra o status operacional de diversos componentes do sistema (como file system e protocolos) usando os LEDs indicadores de status. Também são fornecidos resumos da utilização e capacidade do file system e o status e estatísticas de replicações para replicações de entrada e saída.

A guia **Capacity** mostra dados de diferentes níveis, se aplicável. Se a configuração for um sistema de nível único, haverá somente uma coluna. Se a configuração for um sistema de nível de retenção estendida ou da nuvem, haverá o nível Active, Cloud ou Retention, respectivamente, e colunas de total. Essa guia conterá um gráfico de utilização de capacidade e uma tabela com MTrees no sistema.

A guia **Network** mostra o número total de bytes, bytes de backup e restauração e bytes de replicação de entrada e saída. Há também um gráfico de bytes de rede.

A guia **Charts** permite gerar gráficos de intervalos de tempo selecionados. A guia System Charts tem todos os gráficos do sistema. Para sistemas habilitados para a nuvem, os gráficos estão divididos em duas seções: Historical, que contém os mesmos gráficos de antes; e uma nova seção, Current, que contém dois gráficos de pizza que mostram a distribuição atual dos dados nos sistemas e provedores de nuvem. Esses gráficos são:

- Protection Distribution - um gráfico que exibe a quantidade de dados residentes no local versus em diferentes provedores em nuvem.
- Licensed Capacity Usage - espaço usado em cada provedor, espaço disponível e capacidade total licenciada para todos os provedores juntos.

A guia **Replication** lista as contagens de diferentes pares de replicação automática/sob demanda, tanto de entrada quanto de saída, com aqueles que têm erros ou advertências. Há também gráficos de entrada e saída.

A guia **HA**, para um sistema de alta disponibilidade, contém o diagrama de integridade do sistema de alta disponibilidade, que marca os alertas, quando há, em cada componente do sistema de alta disponibilidade. A seleção de diferentes componentes no diagrama pode filtrar os alertas exibidos na tabela.

Gráficos de recursos

- **CPU utilization** mostra a porcentagem de utilização de CPU para o sistema por data e também mostra quando a limpeza está sendo realizada.
- **Network throughput** mostra se um sistema está enfrentando gargalos relacionados à largura de banda. Você pode determinar quanta largura de banda da rede está sendo usada por sistemas que compartilham a mesma sub-rede para ver se algum está usando mais do que o esperado ou permitido pelos departamentos de TI.

Gráficos do file system

- **Streams counts** mostra os números de cada tipo de fluxo que foi aberto na data e hora indicadas para cada ponto de dados. Não é um agregado (média, mínimo ou máximo) das contagens de fluxos do intervalo selecionado. É mais bem visualizado no menor intervalo (por hora) para que as contagens de fluxos por hora ao longo de cada dia possam ser observadas. Em intervalos maiores (diários ou semanais), somente um único ponto de dados, obtido ao meio-dia, é exibido, o que não é útil para determinar quantos fluxos foram abertos durante o dia ou a semana. Em resumo, o intervalo por hora é a melhor opção para visualizar esse gráfico.
- **Protocol processing** mostra a quantidade de operações por segundo.
- **Protocol throughput** mostra o seguinte:
  - **Data in** é o volume de dados que o file system do DDOS pode ler no buffer do soquete do kernel.
  - **Data out** é o volume de dados que o file system do DDOS pode gravar no buffer do soquete do kernel.
  - **Wait Time per MiB in** é o período que leva para o file system do DDOS receber um mebibyte de dados de um client da rede. Um valor alto indica que o client está enviando dados de modo relativamente lento e é provável que problemas de desempenho estejam relacionados ao client ou à rede. Um valor baixo indica que os dados estão chegando de um client de rede tão rápido quanto ou mais rápido do que eles podem ser desduplicados e gravados no disco.
  - **Wait Time per MiB out** é a medição inversa, a quantidade de tempo que leva para enviar um mebibyte de dados do file system do DDOS para um client de rede. Um valor baixo indica que os dados podem ser enviados pela rede com a mesma rapidez com que estão sendo lidos no disco. Um valor alto indica que os dados estão sendo lidos no disco de modo mais rápido do que podem ser aceitos pela rede e pelo client de rede.

Gráficos de replicação

- O gráfico **Inbound characteristics** mostra as contagens de entradas para os pares de replicação automática e sob demanda.
- O gráfico **Outbound characteristics** mostra as contagens de saídas para os pares de replicação automática e sob demanda.
- O gráfico **Throughput** mostra o throughput para os pares de replicação automática e sob demanda.

Monitorando a replicação

As páginas Replication fornecem detalhes do status e do desempenho sobre os pares de replicação, organizados por sistemas, grupos ou grupos de usuários. Para cada página, você pode visualizar pares, cascatas ou topologia, selecionando os controles no canto superior direito.

NOTA: Para páginas automáticas e sob demanda, a visualização do grupo tem comportamento diferente da visualização do grupo de usuários. A visualização do grupo mostra pares não agrupados enquanto a visualização do grupo de usuários não exibe pares que não pertençam a nenhum grupo de usuários ou unidade de grupo de usuários.

Para Tenants — na página **Replication** > **Overview** > **All Pairs**:

- A hierarquia de agrupamento é grupo de usuários, unidade de grupo de usuários, entrada/saída, automático/sob demanda, par de replicação. Se não houver nenhum par de replicação aplicável, a linha correspondente não será exibida.
- Se uma unidade de tenant não tiver MTrees ou unidades de armazenamento participando como origem ou destino, essa unidade de tenant não será exibida.
- MTrees e unidades de armazenamento que não forem atribuídas a nenhuma unidade de tenant não serão exibidas, mesmo que sejam uma origem ou um destino. Da mesma forma, se todas as unidades de tenant em um tenant não tiverem nenhuma MTree ou unidade de armazenamento com Contextos de replicação, esse tenant não será exibido.
- O RBAC também afeta os tenants e as unidades de tenant que serão exibidos.
- O arquivo CSV (valores separados por vírgulas) contém estas colunas de adição: Tenant, unidade de Tenant, Tenant de origem, unidade de Tenant de origem, Tenant de destino, unidade de Tenant de destino. Ele não contém a coluna System.
- Os pares de replicação são agrupados por tenant ou unidade de tenant a que pertencem os MTrees de origem ou destino ou as unidades de armazenamento.
- Um par será listado duas vezes quando a origem e o destino pertencerem a diferentes unidades de tenant.

Para Tenants — na página **Replication** > **Overview** > **Topology**:

- A origem ou destino mostra o nome da unidade de tenant se o MTree ou a unidade de armazenamento pertencer a uma unidade de tenant.
- As unidades de grupo de usuários são exibidas dentro de sistemas. O nome do tenant é exibido acima do ícone da unidade de tenant.
- As unidades de tenant podem ser expandidas assim como sistemas.
- Os MTrees que não pertencem a uma unidade de tenant são exibidos se uma extremidade do par pertencer a uma unidade de tenant.
- unidades de tenant não atribuídas a um tenant são exibidas se um de seus MTrees ou de suas unidades de armazenamento tiver uma replicação de ou para um MTree ou uma unidade de armazenamento que pertença a uma unidade de tenant.
- Replicações em cascata ainda serão exibidas se incluírem dados que se originam de ou que sejam replicados para uma unidade de tenant gerenciada.
- O menu de contexto para uma unidade de tenant inclui itens do menu para o tenant e lightboxes de detalhes da unidade de tenant.
- Você pode escolher a exibição de pares relacionados para uma unidade de tenant ou um tenant.

- A exibição de pares relacionados de um grupo de usuários exibe todas as unidades de grupo de usuários desse grupo de usuários e a entrada, saída ou pares em cascata de suas unidades de grupo de usuários.

Para Tenants e Systems — na página **Replication** > **Overview** > **All Pairs**:

- Cada sistema DD monitorado ou tenant que tenha configurado pares de replicação fica listado.
- Expanda uma entrada para ver suas replicações de entrada e saída, e para elas, expanda para ver o tipo de replicação: automática (Data Domain ou sistema PowerProtect para replicações do sistema Data Domain ou PowerProtect) e sob demanda (iniciada pelo Client e controlada replicação de arquivos DD Boost) e expanda-os para ver os pares do mesmo tipo. As informações de Entrada e Saída são exibidas somente quando aplicável.
- Use o seletor de coluna para exibir as colunas de status de replicação, o número de pares (valores totais de sistemas, replicações de entrada e saída) e um intervalo de tempo selecionável/configurável para exibir dados históricos de replicação.
- Clique duas vezes em um ícone de erro de status no nível do sistema para abrir a Lightbox de detalhes do sistema, em que, ao passar o mouse sobre o LED de replicação, aparece uma pop-up com um link para a página Alerts, filtrada pelos pares com erro. O ícone de Erro de status de uma categoria (entrada, saída, sistema) mostra se qualquer um de seus itens apresenta uma condição de erro.
- Use o controle de triângulo direito **System** no canto superior esquerdo da tabela para expandir os níveis de entrada e saída para ver todas as Replicações automáticas e sob demanda (se as entradas do sistema ainda não tiverem sido expandidas) e também para reduzir todas as entradas expandidas.

Para Systems, Groups ou Tenants — na página **Replication** > **Automatic**:

- Todas as replicações do sistema monitoradas para replicação de MTree, coleta e diretório são listadas.
- O banner da página exibe a contagem total de replicações Automáticas monitoradas, e a tabela exibe, para cada coluna selecionável do par de replicação, o status, os sistemas de origem e o destino e os dados de desempenho, como tempo de atraso (a célula de atraso fica vermelha quando a duração do atraso for maior ou igual ao limite de Critical e amarela para Warnings; passe o mouse sobre a célula para obter informações detalhadas sobre o limite de intervalo), a tendência de atraso (aumentando: os dados não podem ser replicados dentro do limite de intervalo; estável, diminuindo; ou nenhuma seta se o par estiver suspenso ou com erro), tempo limite (passe o mouse para ver as configurações da política), os bytes restantes e o texto da mensagem de status.
- Entre os controles específicos da página, estão: **Assign Properties** e **Lag Threshold Policy/Manage Lag Threshold Policies** para definir/gerenciar alertas para quando um tempo de intervalo de Replicação automática exceder o limite definido para níveis críticos e de advertência.

Para Systems, Groups ou Tenants — na página **Replication** > **On-Demand**:

- Os dados históricos de replicações concluídas podem ser visualizados em relação às últimas 24 horas, 7 dias, 30 dias, 90 dias ou por meio da configuração de um período personalizado.
- Os detalhes exibidos são para dados replicados Pre-comp que são arquivos replicados, concluídos e com falha, porcentagem de falha e as últimas mensagens de erro.
- Para o modo de exibição do grupo, os dados de pares são totalizados em cada nível de grupo. Os dados de todos os pares estão resumidos na última linha da tabela.
- A quantidade de arquivos concluídos e com falhas pode incluir as replicações de arquivo que o sistema repetiu até quatro vezes devido a falhas recuperáveis. A soma de replicações de arquivos concluídos e com falhas pode ser maior do que a quantidade total de replicações de arquivos que foram iniciadas pelos aplicativos do DD Boost no par de replicação.
- As replicações de arquivo do DD Boost são listadas (para sistemas que executam o DDOS 5.3.1 ou posterior), exibindo para o par: o último status de transferência, as unidades de armazenamento de origem e destino e os dados de desempenho para replicações recentes e concluídas. A tabela pode ser organizada por Pares ou Grupos (alternar no canto superior direito).
- Se os campos de origem ou destino mostrarem um endereço IP em vez de um nome do host, a configuração do servidor DNS para o sistema DD deverá ser modificada. Ao configurar os sistemas DD para monitorar o DD Boost (replicação sob demanda), certifique-se de que seus servidores DNS incluam a configuração para a pesquisa de hostname avançada e inversa. Sem a configuração adequada do servidor DNS, os sistemas DD não poderão traduzir de endereços IP para nomes de host, e os caminhos de origem e destino conterão os endereços IP em vez de nomes de host.
- O controle de replicação **Pair Details** ficará ativo quando um par for selecionado e mostrará muitos detalhes de replicação.
- O controle **System Details** ficará ativo quando uma entrada do sistema for selecionada na página **Overview**.
- O controle **Export CSV file** envia a lista da visão geral com os dados de desempenho dos últimos 7 dias para um arquivo com valores separados por vírgulas (para exibir no Excel, por exemplo).

Visualizando a topologia de replicação para investigar as condições de erro

Quando a visualização **Topology** for selecionada na página **Replication** > **Overview**, ela mostra as relações entre os contextos de replicação configurados do site e utiliza indicadores de status codificados por cores, além de outros controles de mapa para permitir que você localize e aprofunde-se facilmente, a fim de investigar as condições de erro.

Use o menu **Type** para selecionar os tipos de replicação que serão exibidos no ambiente de trabalho do mapa (MTree, diretório, conjunto e arquivos sob demanda). Se um tipo de replicação não for configurado entre as replicações do site, a caixa de seleção no menu será desabilitada. Se um tipo estiver habilitado, mas não selecionado, as relações de nó não aparecem no mapa.

Um slider no mapa controla o escopo de contextos de replicação que são mostrados na exibição do ambiente de trabalho.

A margem interna é uma representação em miniatura do mapa e seu escopo é controlado pela manipulação do slider. A margem interna em si pode ser selecionada e movida ao redor para incluir ou excluir sistemas no ambiente de trabalho do mapa.

Os status de replicação entre sistemas são exibidos com linhas direcionais codificadas por cores, que ficarão vermelhas se qualquer uma das replicações estiver com erro. Passar o mouse sobre a linha mostra o número de pares de replicação e uma contagem de cada nível de status.

Os botões de ação acima do gráfico correspondem ao item selecionado no gráfico. Os itens selecionados podem ser:

- System (botões de detalhes do sistema e de iniciar o DD System Manager serão exibidos).
- Tenant Unit (botões de detalhes do tenant ou da unidade de tenant serão mostrados).
- Property ou Data Set (MTree, diretório, conjunto etc.)

Use os itens de ações para mostrar **Related Items** e **Connected Items** disponíveis para qualquer objeto selecionado no gráfico e para mostrar uma visão aprofundada de todos os pares de replicação que estão configurados. Os itens relacionados em uma seleção incluirão todos os pares com replicações diretas ou com cascatas conectadas aos itens selecionados. O botão **Connected Items** aplicará um filtro para exibir um gráfico conectado com o item selecionado. (Um gráfico estará conectado se existir um caminho entre cada par de nós do gráfico).

O painel direito lista os **Replicated Pairs** (de sistemas destacados no ambiente de trabalho do mapa ou de todos os contextos se nada estiver destacado), mostrando o tipo de contexto, sistemas de origem e destino, status, com um link para obter mais detalhes. A seleção de um contexto ativa o controle **Pair Details**.

Verificando a lightbox Replication Pair Details

A seleção de um par de replicação em qualquer uma das páginas Replication ative o controle **Pair Details**, que abre a *lightbox Replication Pair Details*.

Há duas guias: Overview e Charts.

A guia **Overview** mostra:

- o último status de transferência
- os sistemas de origem e destino
- configurações, como criptografia e status operacional
- Ícones codificados por cores mostrando os níveis de capacidade

A guia **Charts** fornece gráficos para:

- Características de pares - fatores de desempenho, como gravados pré-compactação, replicados pré-compactação, replicação pós-compactação, restantes pré-compactação, bytes de rede e taxa de compactação.
- Tendência de atraso - gráficos restantes pré-compactação, atraso de replicação, gravados pré-compactação, limite de advertência e limite crítico (não disponíveis para replicação sob demanda)
- Utilização da CPU
- Dados gravados
- Throughput de rede e replicação
- Características de origem e destino, e pares comuns

Os gráficos são alinhados verticalmente para sistemas de origem e destino, pelo mesmo intervalo de tempo, permitindo comparações de ambos os sistemas em qualquer point-in-time.

Possíveis razões para a mensagem "SU is unresolved"

Se uma unidade de armazenamento de um par de replicação do DD Boost mostrar a mensagem "SU is unresolved", estes são alguns motivos possíveis:

- O sistema remoto não está registrado com o DDMC.
- Ambos os sistemas estão registrados, mas um está executando uma versão incompatível do DDOS e não é capaz de relatar o nome da unidade de armazenamento.
- O nome de host remoto é um endereço IP e não pode corresponder a um nome de host registrado.

Monitorando o status com relatórios

Os relatórios compilam as informações de áreas de interesse em sistemas gerenciados e do Secure Multi-Tenancy (SMT) e DD Cloud Tier.

Os relatórios são gerados com base nos tipos de modelo do relatório padrão. Os modelos de relatório configuram o agendamento, o conteúdo e a distribuição via e-mail do relatório.

NOTA: Se um usuário que é o "proprietário" de qualquer modelo de relatório for excluído da CLI, esses modelos de relatório ainda serão exibidos como pertencentes ao usuário "excluído", mas os relatórios não serão mais executados nos períodos agendados.

Existem três tipos de modelo de relatório padrão para os sistemas:

- Capacidade (Capacity Overview)
- Replicação (Replication Status)
- Status (Current Health Status)

Há dois tipos de modelo de relatório padrão para SMT e Cloud Tier:

- Status (Daily Status)
- Utilização (Usage Metrics)

Criando um relatório com o assistente

O assistente Add Report Template cria um modelo de relatório para uso na execução de relatórios sobre os principais pontos de dados.

Sobre esta tarefa

NOTA: O número de amostras de medição de capacidade física que são apresentadas pelo DDMC é geralmente diferente do número de amostras que são exibidas pelo DDOS. O DDMC exibe mais amostras porque ele não faz nenhuma limpeza de amostras de medição de capacidade física. O DDOS limpa as amostras históricas de medição de capacidade física para MTrees, unidades de grupo de usuários e grupos de usuários diariamente e mantém a distribuição das amostras históricas por não mais que uma amostra por hora no período dos últimos 90 dias; depois não mais do que uma por dia no período do último ano; e por fim, não mais do que uma por semana nos últimos 10 anos.

Etapas

1. Selecione **Reports** > **Management**.
2. Selecione Add (sinal de mais verde).
3. Na caixa de diálogo Add Report Template, selecione o tipo de relatório que deseja (System Reports, Multitenancy Reports ou Cloud Tier Reports) e selecione **Next**.
4. Digite um nome e selecione um modelo. Escolha uma ou mais seções para incluir e selecione **Next**.
   a. Para o sistema, as opções são Capacity, Replication ou Status.

      A caixa de seleção **Hide capacity projection data** é exibida depois de um **Template** ser selecionado na lista suspensa. A marcação dessa caixa de seleção oculta os dados de projeção do relatório.
   b. Para o Multi-Tenancy, as opções são Status ou Usage.
   c. Para Cloud Tier, as opções são Status ou Usage.
5. De acordo com sua seleção entre System, Multi-Tenancy ou Cloud Tier:
   a. Sistema: selecione um filtro para restringir o escopo dos objetos relatados (por exemplo, filtrar por grupos selecionados). Selecione o intervalo de tempo para coleta de dados (por exemplo, últimas 24 horas) e a retenção do relatório (por exemplo, 7 dias). Selecione **Edit** para definir um agendamento para a frequência e a hora em que o relatório é executado. A hora de geração do relatório será duas horas após a hora *Starts On*. Selecione **Next**.
   b. Multi-Tenancy: Selecione um escopo (**Tenant Unit** ou **Tenant**). O relatório Daily Status está sempre configurado para mostrar as últimas 24 horas de dados históricos e você pode selecionar a retenção do relatório (sempre, 7 dias, 30 dias, 90 dias). O relatório Usage Metrics (que é gerado como uma planilha do Excel) permite que você exiba dados para um mês completo ou uma semana completa. Selecione **Edit** para definir um agendamento para a frequência e a hora em que o relatório é executado. A hora de geração do relatório será duas horas após a hora *Starts On*.
   c. Relatórios Cloud Tier: selecione **Cloud Service Providers** para filtrar os sistemas que possuem nível de nuvem configurada para conectá-los.
6. Opcionalmente, adicione endereços de e-mail do destinatário (para quando o relatório for concluído e se ocorrer um erro). Para o modelo de relatório do Tenant Unit, as mensagens de e-mail do administrador de Tenant Unit são adicionadas por padrão. Para

o modelo de relatório de tenant, o e-mail do administrador de tenant é adicionado por padrão. Você pode adicionar ou remover manualmente essas mensagens de e-mail. Selecione **Next**.

7. Analise os detalhes e selecione para salvar o modelo para uso posterior e para executar o relatório imediatamente. Selecione **Finish**.

Resultados

Depois de ter sido criado, um modelo de relatório é adicionado como uma entrada na tabela de relatórios. Quando selecionado, o modelo de relatório pode ser usado para executar imediatamente um relatório ou pode ser editado ou excluído, ou a hora em que foi executado pela última vez pode ser exibida.

Editar relatório

As propriedades de um modelo de relatório existente podem ser editadas.

Etapas

1. Selecione **Reports** > **Management**.
2. Selecione um nome de modelo e clique em Edit.
3. Na caixa de diálogo Edit Report Template, escolha a propriedade de relatório a ser editada.
   - Conteúdo - nome do modelo, modelo usado e seções.
   - Escopo - sistemas no relatório.
   - Programação - status, período, agendamento de tempo de execução e retenção de relatórios.
   - E-mail - adicione e exclua endereços de e-mail em que os relatórios são enviados quando o relatório foi concluído e houve um erro. Os relatórios de capacidade têm a opção de ter o conteúdo incorporado no e-mail. Por padrão, o relatório é enviado como um anexo de e-mail.

Gerando um relatório imediatamente

Para gerar um relatório imediatamente, selecione um modelo de relatório listado na tabela de nomes modelo e, em seguida, **Run Report**.

Um relatório (denominado pela concatenação do registro de data para o título do modelo) é criado e aberto como um arquivo PDF em seu navegador, exceto para os relatórios de utilização do tenant e de uso da nuvem, que geram um arquivo .xlsx.

As informações de geração de relatório são listadas na tabela Report History, em que ele pode ser visualizado, renomeado ou excluído.

Limpando relatórios de usuários excluídos

Modelos de relatório pertencentes a usuários excluídos podem ser excluídos ou reatribuídos a outro usuário do DDMC.

Os usuários também podem ser excluídos na janela **Settings** > **Access** > **Local Users**.

Ao excluir um usuário local, o DDMC fornece a opção de selecionar outro usuário local para atribuir os modelos de relatório do usuário excluído ou excluir os modelos de relatório, juntamente com seu proprietário. Os modelos de relatório são reatribuídos ao sysadmin por padrão, mas qualquer usuário local pode ser selecionado.

Se os modelos de relatório forem reatribuídos, os agendamentos de relatórios são desabilitados por padrão até que os destinatários do e-mail do relatório sejam atualizados. Os modelos de relatório podem ser atualizados na janela **Report Management** ou no botão **Edit** na guia **Schedule**.

5

Gerenciando sistemas de DD

Tópicos:

- Visualizando o DD System Manager
- Atualizando o software do sistema
- Usuários locais

Visualizando o DD System Manager

Em algumas páginas do DDMC, você pode iniciar uma sessão do DD System Manager para realizar a configuração ou uma solução de problemas. A versão iniciada do DD System Manager é executada no DDMC e não no sistema, oferecendo, assim, administração centralizada, segura e simultânea para diversos sistemas.

Para iniciar uma sessão, selecione uma entrada em uma lista da tabela (por exemplo) e selecione **View DD System Manager** em qualquer uma das seguintes páginas do DDMC:

- **Health** > **Status**
- **Sistemas de** > **Capacidade**
- **Gerenciamento de** > **Capacidade** (visualização clássica)
- **Capacidade** > **Projetada** (visualização clássica)
- **Infrastructure** > **Systems**
- Lightbox **Replication Pair Details**
- Lightbox **System Details**

A sessão do DD System Manager que é iniciada não requere nenhum log-in ou log-out e fornece gerenciamento completo do sistema. O DD System Manager abre exibindo a área correspondente de onde ele foi iniciado (por exemplo, se a inicialização foi na visualização Alerts, a página Alerts no sistema Data Domain será aberta).

NOTA: Em **Classic view**, o DD System Manager é aberto em uma nova janela. Certifique-se de que o bloqueador de pop-up de seu navegador esteja configurado para permitir pop-ups para o DDMC.

O DD System Manager iniciado é exibido no DDMC, e o menu de navegação é alterado para o menu do DD System Manager. No canto superior esquerdo, há um botão **Back** com o nome do sistema mostrado abaixo. Ao clicar no botão **Back**, você retorna para o módulo do DDMC que iniciou o DD System Manager.

Observe o seguinte sobre como iniciar o DD System Manager no DDMC:

- Você pode **visualizar o DD System Manager** para um sistema no qual tenha uma função de *admin*, *limited-admin* ou *user*.
- Uma permissão consiste em um sistema ou grupo, um usuário (local ou NIS) e uma função.
  - A função de administrador é necessária para a configuração de replicação e configuração de IPMI (Intelligent Platform Management Interface).
- O inventário de sistemas no DDMC é usado.
  - Os sistemas mostrados são baseados em permissões efetivas.
  - Apenas sistemas de origem e destino de replicação registrados com o DDMC são mostrados.
- Outras portas de firewall para a sessão não precisam ser abertas. Depois que um sistema é adicionado ao DDMC, as atribuições de porta existentes são usadas para a conexão do DD System Manager.

Atualizando o software do sistema

Procedimento

NOTA: Sistemas de alta disponibilidade não podem ser atualizados do DDMC. Inicie o DD System Manager para visualizar o sistema de alta disponibilidade e realize a atualização no próprio sistema.

1. Obtenha um pacote de atualização do DDOS fazendo download de um pacote de atualização no site de suporte on-line.

2. Faça upload do pacote de atualização do DDOS no inventário do DDMC.
3. Execute a atualização do DDOS nos sistemas.

Gerenciar pacotes de atualização do sistema

Para poder atualizar um sistema através do DDMC, você precisa fazer upload do pacote de atualização para o DDMC. O administrador do DDMC pode gerenciar pacotes (adicionar e excluir) na guia **PACKAGES**.

Etapas

1. Selecione **Infrastructure** > **Updates**.
   Agora, há duas guias disponíveis na janela principal: **Systems** e **Packages**.
2. Selecione **Packages**.
3. Clique em **ADD** para adicionar um pacote de software.
   Depois que o pacote de atualização tiver sido carregado para o DDMC, você pode fazer atualizar um ou mais sistemas.
   NOTA: Para excluir um pacote, marque a caixa ao lado do nome de um pacote e clique em **DELETE** para remover esse pacote de software.

Fazendo atualização no sistema

O DDOS em um ou mais sistemas DD pode ser atualizado do DDMC com uma operação de atualização. Se os sistemas não estiverem em um estado gerenciado aceitável (por exemplo, inacessível, suspenso, atualizando), a ação de atualização fica indisponível.

Sobre esta tarefa

NOTA: Por motivos de segurança, há um limite de tempo de 30 minutos para o upload de pacotes de RPM para atualizações dos sistemas DDMC e DD usando a GUI do DDMC. Se você tiver uma conexão lenta de uma máquina client para o DDMC e o upload demorar mais de 30 minutos, a conexão será cancelada e você não poderá usar o DDMC para fazer upload do pacote.

Solução temporária: Use a CLI para fazer upload do pacote no DDMC (por exemplo, use `SCP/PSCP` a partir de um terminal do Unix ou Windows CMD).

Para atualizações dos sistemas DD e DDMC, faça o carregamento do pacote para `/ddr/var/releases`.

Etapas

1. Selecione **Infrastructure** > **Updates**.
   Agora, há duas guias disponíveis na janela principal: **SYSTEMS** e **PACKAGES**. **SYSTEMS** é selecionado automaticamente e uma lista de sistemas disponíveis para atualização é exibida.
2. Seleciona um ou mais sistemas a serem atualizados.
   Se houver um erro de pré-verificação, há uma opção para executar a pré-verificação manualmente a partir do painel de detalhes depois da corrigir qualquer erros.
3. Clique no botão **Configure Update**.
   NOTA: Sistemas de alta disponibilidade não podem ser atualizados do DDMC. Se um ou mais sistemas de alta disponibilidade forem selecionados, o DDMC exibirá uma mensagem informando que não há suporte para atualizações de sistemas de alta disponibilidade.
4. Digite o nome da programação de atualização e selecione uma das opções a seguir.
   - **Download Package Only** - permite o download prévio de um pacote de atualização para os sistemas sem instalação.
   - **Install Update Only** - Instalação de pacotes de atualização baixados previamente em sistemas.
     NOTA: Essa opção só está disponível para sistemas com pacotes com download prévio feito com sucesso.
   - **Download Package and Install Update**- permite configurar o download e a instalação de um pacote de atualização para sistemas selecionados.

Como agendar uma atualização de software

A distribuição e a instalação de pacotes RPM do sistema DD podem ser agendadas para qualquer data futura.

Sobre esta tarefa

Essas atualizações podem ser configuradas de acordo com um sistema DD individual ou horário de DDMC.

NOTA: Se uma ação agendada tiver sido iniciada em um sistema, o agendamento pode ser excluído mesmo se estiver em andamento. Uma vez que um agendamento esteja em andamento, ele pode ser excluído, mas não editado. Um agendamento de atualização do sistema pode ser excluído mesmo se estiver em andamento.

NOTA: A hora e a data selecionadas para o agendamento são validadas em relação ao fuso horário do navegador para determinar se a seleção se trata de uma data e hora antigas. Se a data/hora atual for considerada com base no horário do navegador, a seguinte mensagem de advertência pode ser exibida:

```
Aviso: o horário selecionado está no passado para um ou mais sistemas. Escolha um tempo no futuro para acomodar todos os fusos horários do sistema.
```

Etapas

1. Clique em **Configure Update**.
2. Digite um **Update Name**.
3. Selecione **Download Package Only**, **Install Update Only**, ou **Download Package and Install Update**.
   - **Download Package Only**: permite o download de um pacote de atualização para os sistemas sem instalação
   - **Install Update Only**: instalação de pacotes de atualização baixados anteriormente nos sistemas (esta opção só está disponível para sistemas com pacotes baixados anteriormente bem-sucedidos. A atualização pode acionar a reinicialização do sistema.)
   - **Download Package and Install Update**: permite configurar o download e a instalação de um pacote de atualização para sistemas selecionados (a atualização pode acionar a reinicialização do sistema.)

   NOTA: Verifique a matriz de compatibilidade antes de iniciar a instalação da atualização.
4. Clique em **Next**.
5. Selecione na lista de sistemas disponíveis a atualização configurada.

   NOTA: Os sistemas que são de alta disponibilidade (HA) ou que tenham um agendamento de atualização existente não podem ser atualizados e não aparecem na lista de sistemas disponíveis.
6. Clique em **Next**.
7. Selecione o pacote a ser aplicado ao sistema ou aos sistemas selecionados anteriormente.
8. Clique em **Next**.
9. Selecione quando executar os downloads e atualizar, **Now** ou **Later**.

   Se for escolhido **Later**, selecione se deseja usar a hora do sistema ou a hora do DDMC e agende a data e a hora específicas.
10. Clique em **Next**.
11. Analise o resumo e, se aplicável, selecione **Reboot before instalation**.

    Uma reinicialização do sistema permite que a atualização continue sem conflitos com processos em execução em segundo plano e pode ser necessária para algumas atualizações.
12. Clique em **Finish**.

Usuários locais

Usuários locais são usuários não administrativos que podem fazer log-in no DDMC, mas podem apenas visualizar os sistemas especificados por um administrador.

Criando acesso para usuários

Para configurar o acesso ao DDMC, você deve adicionar usuários e grupos de acesso e adicionar permissões para determinadas funções.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Local Users**.
2. Clique em **Add** para criar usuários.

Esses usuários podem fazer log-in no DDMC, mas não podem ver nenhum outro sistema. Você pode adicionar permissões para visualizar (função user), administrar (função admin ou admin limitado) ou criar snapshots (backup operator) a grupos e sistemas.

Grupos de usuários têm funções de admin ou de user; funções de usuário podem ser admin, limited-admin e user. Se um usuário ou um grupo de usuários tiver a função de admin, eles poderão visualizar todos os sistemas DD por padrão; *não é necessário definir outras permissões para usuários e grupos admin.*

3. **Access Authentication** para criar grupos de acesso (NIS, Windows (usando Workgroup ou Active Directory) e LDAP) no DDMC.
4. Para usuários e grupos de usuários com a função de usuário, é preciso definir permissões nos sistemas para que eles possam visualizar os sistemas. Selecione **Administration** > **Permissions**.
5. Selecione Add (sinal de mais verde).
6. Na caixa de diálogo Add Permissions, selecione o local para adicionar a permissão:
   - **Add permissions to systems** — selecione essa opção e, na lista de sistemas gerenciados, selecione as caixas de seleção dos sistemas nas quais as permissões serão atribuídas.
   - **Add permissions to groups** — selecione essa opção e, na lista de grupos, selecione as caixas de seleção dos grupos nas quais as permissões serão atribuídas.
7. Na área User, selecione Add (sinal de mais verde), selecione um ou mais usuários na caixa de diálogo Select Users e clique em **Select**.
8. Clique no campo Role do usuário e selecione a função de acesso: Administrator, Limited-Admin, Backup Operator ou User.
9. Selecione Add (sinal de mais verde).

   Os usuários recebem a função atribuída (Administrator, Limited-Admin, Backup Operator ou User) para os sistemas ou grupos selecionados.

Próximas etapas

Para simplificar o gerenciamento de permissões:

- É recomendável que o uso da função de administrador para o DDMC seja mínimo.
  - A função admin pode gerenciar todos os sistemas Data Domain no inventário do DDMC. Além disso, o administrador do DDMC configura as propriedades e grupos do DDMC e atribui suas permissões.
  - Configure a maioria dos logins para o DDMC com a função de usuário.
- Use grupos de usuário do NIS para permissões, pois simplifica o processo de adicionar, remover e modificar usuários sem alterar a atribuição de permissões.
- Use grupos do sistema DD para permissões em vez de atribuir permissões a sistemas individuais.

  Atribuindo permissões no nível do grupo, as permissões com base em políticas podem ser usadas com um modelo de união que é aplicado à hierarquia do grupo inteiro.

- Inicie com permissões de nível inferior na parte superior da hierarquia:
  - Atribua permissões de nível inferior na raiz da hierarquia do grupo.
  - Atribua permissões de nível superior na folha da hierarquia do grupo.
  - Use um modelo de união, não um modelo de sobreposição. Isso facilita alterar as permissões em níveis inferiores sem afetar toda a hierarquia.

Verifique as alterações:

- Após a atribuição de permissões ou alteração da lista de membros do grupo, verifique a alteração, observando a função Effective de um sistema.

Use Administração central:

- Use o DDMC para administrar centralmente todos os sistemas, reduzindo o uso de contas locais em cada sistema gerenciado. Desative o acesso direto da interface de usuário a sistemas gerenciados pelo DDMC.

Noções básicas sobre as permissões do DDMC

As páginas **Administration** > **Permissions** (Assigned, Groups, Systems, Users) mostram as permissões de usuários do DDMC por função atribuída.

As permissões são um "triângulo" de três componentes:

- o objeto gerenciado (groups ou systems)
- o usuário (local, NIS, LDAP ou Active Directory)
- a função do DD System Manager (Administrator, Limited-Admin, Backup Operator ou User)

As páginas de permissões também são usadas para adicionar, modificar e remover as permissões de grupos e sistemas. Cada uma das exibições mostra os usuários, suas funções atribuídas e suas funções efetivas.

6

Administrando o Multi-tenancy seguro

Tópicos:

- Como o DDMC ajuda no monitoramento do SMT
- Criar e gerenciar tenants
- Criar e gerenciar unidades do tenant
- Criando, editando e gerando relatórios do SMT

Como o DDMC ajuda no monitoramento do SMT

O DDMC pode configurar e monitorar o Secure Multitenancy (SMT) para armazenamento de backup e replicação do DD Boost em vários sistemas Data Domain.

Em um ambiente multitenant seguro, os administradores de armazenamento (*locadores*) e os administradores de backup (*tenants*) cooperam para alocar e gerenciar o armazenamento, conforme segue:

NOTA: O Secure Multitenancy não é compatível com instâncias do DDVE 2.0, mas é compatível com o DDVE 3.0 e versões posteriores.

1. O administrador de armazenamento cria tenants no DDMC.

   Por exemplo, o administrador de armazenamento em uma organização de TI corporativa pode criar um tenant para o administrador de backup no departamento financeiro.

2. O administrador de armazenamento cria uma ou mais unidades de tenant nos sistemas para servir como contêineres virtuais para cada tenant.
3. O administrador de armazenamento cria um ou mais MTrees ou unidades de armazenamento do DD Boost.
4. O administrador de backup configura o software para backup para usar os MTrees na unidade de tenant como destinos de armazenamento.

Para obter mais informações, consulte o capítulo "Secure Multitenancy" do *DDOS Administration Guide*.

Visão geral do Secure Multitenancy

O *Secure Multitenancy (SMT)* do Data Domain é a hospedagem simultânea, por um departamento de TI interno ou um provedor externo, de uma infraestrutura de TI para mais de um consumidor ou carga de trabalho (unidade de negócios, departamento ou grupo de usuários).

O SMT proporciona a capacidade de isolar com segurança muitos usuários e cargas de trabalho em uma infraestrutura compartilhada, para que as atividades de um tenant não apareçam ou fiquem visíveis aos outros tenants.

Um *tenant* é um consumidor (unidade de negócios, departamento ou cliente) que mantém uma presença persistente em um ambiente hospedado.

Em uma empresa, um tenant deve consistir em uma ou mais unidades de negócio ou departamentos em um sistema de proteção configurado e gerenciado pela equipe de TI.

- Para o caso de uso de uma unidade de negócios (UN), os departamentos de Recursos Humanos e Financeiro de uma corporação podem compartilhar o mesmo sistema, mas cada departamento não reconhecerá a presença do outro.
- Para um caso de uso de prestador de serviços (PS), o PS deve implementar um ou mais sistemas para acomodar diferentes serviços de Armazenamento de proteção para vários clientes finais.

Ambos os casos de uso enfatizam a separação de diferentes dados de cliente no mesmo sistema físico.

Terminologia usada no Multi-Tenancy seguro (SMT)

As noções básicas sobre a terminologia usada no SMT ajudarão você a entender melhor esse ambiente exclusivo.

MTrees

MTrees são partições lógicas do file system e oferecem o mais alto grau de granularidade de gerenciamento, indicando que os usuários podem executar operações em um MTree específico sem afetar o file system inteiro. MTrees são atribuídos às unidades de tenant e contêm as configurações individualizadas da unidade de tenant para gerenciamento e monitoramento do SMT.

Multi-tenancy

Multi-tenancy refere-se à hospedagem de uma infraestrutura de TI por um departamento de TI interno, ou um provedor externo de serviços, para mais de um consumidor/carga de trabalho (unidade de negócios/departamento/tenant) simultaneamente. O DD SMT ativa a *Proteção de dados como serviço*.

RBAC (controle de acesso baseado em função)

O *RBAC* oferece diversas funções com diferentes níveis de privilégio, que se combinam para proporcionar isolamento administrativo em um sistema de proteção multi-tenant.

Storage Unit

Uma *Unidade de armazenamento* é um MTree configurado para o protocolo DD Boost. O isolamento de dados é alcançado ao criar uma unidade de armazenamento e atribuí-la ao usuário do DD Boost. O protocolo do DD Boost permite acessar somente as unidades de armazenamento atribuídas aos usuários do DD Boost conectados ao sistema.

Tenant

Um *tenant* é um consumidor (unidade de negócios/departamento/cliente) que mantém uma presença persistente em um ambiente hospedado.

Autoatendimento do tenant

O *Autoatendimento do grupo de usuários* é um método para permitir que um grupo de usuários faça log-in em um sistema de proteção para realizar alguns serviços básicos (visualizar MTrees ou unidades de armazenamento que pertencem à unidade de grupo de usuários, ou alterar a senha do grupo de usuários). Isso reduz o gargalo de sempre ter de passar por um administrador para essas tarefas básicas. O tenant pode acessar somente suas unidades de tenant atribuídas. Usuários de tenant e Administradores de tenant terão privilégios diferentes.

Unidade de tenant

Uma *unidade de tenant* é a partição de um sistema que serve como a unidade de isolamento administrativo entre tenants. Unidades de tenant atribuídas a um tenant podem estar nos mesmos sistemas ou em sistemas diferentes e são fixadas e logicamente isoladas umas das outras, o que garante a segurança e o isolamento do caminho de controle ao executar vários tenants simultaneamente na infraestrutura compartilhada. Unidades de tenant podem conter um ou mais *MTrees*, os quais detêm todos os elementos de configuração necessários em uma configuração de multi-tenancy. Usuários, grupos de gerenciamento, grupos de notificação e outros elementos de configuração são parte de uma unidade de tenant.

Noções básicas sobre o RBAC no SMT

No Secure Multitenancy (SMT), a permissão para realizar uma tarefa depende da função atribuída a um usuário. O DDMC utiliza o controle de acesso baseado em função (RBAC) para controlar essas permissões.

Todos os usuários do DDMC podem:

- Visualizar todos os tenants
- Criar, ler, atualizar ou excluir unidades de tenant que pertencem a qualquer tenant se o usuário for um administrador no sistema que hospeda a unidade de tenant
- Atribuir e cancelar a atribuição de unidades de tenant para e de um tenant se o usuário for um administrador no sistema que hospeda a unidade de tenant

- Visualizar as unidades de tenant que pertencem a qualquer tenant se o usuário tiver qualquer função atribuída no sistema que hospeda a Unidade tenant

A realização de tarefas mais avançadas depende da função do usuário, conforme segue:

função admin

Um usuário com função *admin* pode realizar todas as operações administrativas em um sistema de proteção. Um *admin* também pode realizar todas as operações administrativas do SMT no sistema, inclusive instalar um SMT, atribuir funções para o usuário SMT, ativar o modo de autoatendimento do tenant, criar um tenant, e assim por diante. No contexto do SMT, o *admin* é normalmente conhecido como o *proprietário*. No DDOS, a função é conhecida como o *sysadmin*.

Para ter permissão para editar ou excluir um grupo de usuários, você deve ser um *admin* do DDMC e um *sysadmin* do DDOS em todos os sistemas associados a unidades de grupos de usuários daquele grupo de usuários. Se o tenant não tiver nenhuma unidade de tenant, você precisa apenas ser um *admin* do DDMC para editar ou excluir aquele tenant.

Função limited-admin

Um usuário com uma função *limited-admin* pode realizar todas as operações administrativas em um sistema Data Domain como *admin*. No entanto, usuários com a função *limited-admin* não podem excluir ou destruir MTrees. No DDOS, há uma função equivalente de *limited-admin*.

função admin-tenant

Um usuário com uma função *admin-tenant* pode realizar certas tarefas apenas quando o modo *autoatendimento do tenant* estiver ativado para uma unidade de tenant específica. As responsabilidades incluem agendar e executar um aplicativo de backup para o tenant e monitorar os recursos e estatísticas dentro da Unidade de tenant atribuída. O *admin-tenant* pode visualizar registros de auditoria, mas o RBAC garante que apenas registros de auditoria das unidades de tenant que pertencem ao *admin-tenant* estejam acessíveis. Além disso, o *admin-tenant* garante a separação administrativa quando o modo de autoatendimento do tenant for habilitado. No contexto do SMT, o *admin-tenant* geralmente é conhecido como *admin de backup*.

função de usuário do tenant

Um usuário com função de *tenant-user* pode monitorar o desempenho e utilização de componentes do SMT apenas em unidade(s) de tenant atribuídas a eles e apenas usando autoatendimento se o tenant estiver ativado, mas um usuário com essa função não pode visualizar registros de auditoria de suas unidades de tenant atribuídas. Além disso, *usuários de grupo de usuários* podem executar os comandos `show e list`.

nenhuma função

Um usuário com função de *nenhum* não tem permissão para realizar nenhuma operação em um sistema que não seja alterar sua senha e acessar os dados usando o DD Boost. No entanto, depois que o SMT é ativado, o *admin* pode selecionar um usuário com função *nenhum* do sistema e atribuir a ele uma função específica do SMT de *admin-tenant* ou *usuário do tenant*. Então, esse usuário pode realizar operações nos objetos de gerenciamento do SMT.

Grupos de gerenciamento

BSPs (prestadores de serviços de backup) podem usar *grupos de gerenciamento* definidos em um AD (active directory) único e externo ou NIS (Serviço de informação da rede) para simplificar o gerenciamento das funções dos usuários nas unidades de tenant. Cada tenant do BSP pode ser uma empresa separada e externa e pode usar um nome de serviço como AD ou NIS.

Com os grupos de gerenciamento do SMT, os servidores do AD e NIS são instalados e configurados pelo *admin* da mesma maneira que os usuários locais do SMT. O *admin* pode solicitar ao seu administrador do AD ou NIS para criar e preencher o grupo. O *admin* então atribui uma função do SMT para o grupo inteiro. Qualquer usuário do grupo registrado no sistema é registrado com a função atribuída ao grupo.

Quando os usuários deixam ou entram em uma empresa tenant, eles podem ser removidos ou adicionados ao grupo pelo administrador do AD ou NIS. Não é necessário modificar a configuração do RBAC em um sistema quando os usuários que fazem parte do grupo forem adicionados ou removidos.

Tabela de permissão de tenant e de unidade de tenant

As permissões para trabalhar com tenants e unidades de tenant dependem da função do usuário no DDMC e no sistema (DDOS).

Tabela 11. Tabela de permissão para tenants e unidades de tenant, admin e limited-admin do DDMC

Função de usuário do DDMC/DDOS	Administrador do DDMC/ sysadmin do DDOS	Administrador limitado do DDMC/sysadmin do DDOS
Tenant		
Criar tenant	yes	yes
Editar/excluir tenant sem nenhuma unidade de tenant	yes	yes
Excluir/destruir MTree	yes	não
Editar/excluir tenant com unidades de tenant[a]	yes	yes
Visualizar todos os tenants definidos no DDMC	yes	yes
Exibir problema com unidades de tenant para o tenant na página de resumo	yes	yes
Visualizar lightbox Tenant Details	yes	yes
Visualizar problemas de configuração do MTree para o tenant na página de resumo	yes	yes
Unidade de tenant		
Consultar o sistema para seleção no Assistente de criação de unidade de tenant	yes	yes
Editar e excluir unidade de tenant	yes	yes
Visualizar as unidades de tenant associadas aos sistemas listados na página do inventário	yes	yes
Editar/excluir unidade de tenant não gerenciada	yes	yes
Atribuir/cancelar a atribuição de unidade de tenant para/do tenant	yes	yes
Visualizar lightbox Tenant Unit Details	yes	yes

a. O admin ou o limited-admin do DDMC deve ter a função de sysadmin ou limited-admin do DDOS em todos os sistemas DD que hospedam as unidades de tenant do tenant.

Tabela 12. Tabela de permissão para tenants e unidades de tenant, usuário do DDMC

Função de usuário do DDMC/DDOS	Usuário do DDMC/ sysadmin ou limited-admin do DDOS	Usuário do DDMC/usuário ou operador de backup do DDOS	Usuário do DDMC/ nenhuma função do DDOS
Tenant			
Criar tenant	não	não	não
Editar/excluir tenant sem nenhuma unidade de tenant	não	não	não
Excluir/destruir MTree	não	não	não
Editar/excluir tenant com unidades de tenant	não	não	não
Visualizar todos os tenants definidos no DDMC	yes	yes	yes
Exibir problema com unidades de tenant para o tenant na página de resumo *	yes	yes	não
Visualizar lightbox Tenant Details *	yes	yes	não

Tabela 12. Tabela de permissão para tenants e unidades de tenant, usuário do DDMC (continuação)

Função de usuário do DDMC/DDOS	Usuário do DDMC/ sysadmin ou limited-admin do DDOS	Usuário do DDMC/usuário ou operador de backup do DDOS	Usuário do DDMC/ nenhuma função do DDOS
Visualizar problemas de configuração do MTree para o tenant na página de resumo *	yes	yes	não
Unidade de tenant			
Consultar o sistema para seleção no Assistente de criação de unidade de tenant	yes	não	não
Editar e excluir unidade de tenant	yes	não	não
Visualizar as unidades de tenant associadas aos sistemas listados na página do inventário	yes	yes	não
Editar/excluir unidade de tenant não gerenciada	yes	não	não
Atribuir/cancelar a atribuição de unidade de tenant para/do tenant	yes	não	não
Visualizar lightbox Tenant Unit Details	yes	yes	não

* Para usuários do DDMC, apenas agregar/mostrar unidades de tenant do tenant no sistema DDOS para as quais o usuário DDMC tem uma função do DDOS (sysadmin, limited-admin, user ou backup operator)

Casos de uso do SMT

Os casos de uso a seguir resumem como o Secure Multitenancy (SMT) pode ser implementado em infraestruturas de armazenamento de proteção.

Backup local

Em um caso de uso de backup local, uma infraestrutura de armazenamento de proteção é compartilhada entre clients, e a implementação é local para a empresa. A equipe de TI no local usa cada unidade de tenant para fazer backup dos dados de uma unidade de negócios específica.

Backup replicado

Em um caso de uso de backup replicado, o tenant realiza backups locais em seu local físico, mas não deseja ter ou gerenciar um site remoto para fins de recuperação de desastres. Para esse tipo de tenant, os provedores de serviços podem hospedar vários tenants, sendo que cada um replica sua própria unidade de tenant, para fornecer serviços de backup replicado em uma plataforma de dispositivo de backup compartilhada do Data Domain.

Backup remoto

Em um caso de uso de backup remoto, um client não realiza backups locais no local físico. Em vez disso, o client executa backups diretos via WAN em um ambiente de TI de backup hospedado gerenciado por um provedor de serviços ou um provedor de serviço hospedado. O backup remoto é usado para o backup tradicional baseado no client e o backup direto do aplicativo.

DD Boost de usuários múltiplos e unidades de armazenamento no SMT

Ao utilizar o DD Boost de usuários múltiplos com o Secure Multitenancy (SMT), as permissões do usuário são definidas pela propriedade da unidade de armazenamento.

O *DD Boost de usuários múltiplos* se refere ao uso de múltiplas credenciais do usuário do DD Boost para controle de acesso do DD Boost, no qual cada usuário possui um nome do usuário e senha separados.

Uma *Unidade de armazenamento* é um MTree configurado para o protocolo DD Boost. Um usuário pode ser associado a, ou "ser proprietário," de uma ou mais Unidade de armazenamento. As Unidades de armazenamento que pertencem a um usuário não podem pertencer a outro usuário. O usuário que possui a unidade de armazenamento pode acessar a mesma para qualquer tipo de acesso aos dados, como backup/restauração. O número de nomes de usuários do DD Boost não pode exceder o número máximo de MTrees. (Consulte o capítulo "MTrees" neste guia para o atual número máximo de MTrees para cada modelo.) Unidades de armazenamento que estão associadas a SMT devem ter a função *none* atribuída a elas.

Cada aplicativo de backup deve ser autenticado usando seu nome de usuário e senha do DD Boost. Após a autenticação, o DD Boost verifica as credenciais autenticadas para confirmar a propriedade da Unidade de armazenamento. É concedido ao aplicativo de backup o acesso à unidade de armazenamento apenas se as credenciais do usuário apresentada pelo aplicativo de backup corresponderem aos nomes do usuário associados com a unidade de armazenamento. Se as credenciais do usuário e os nomes de usuário não corresponderem, o trabalho apresenta falha com um erro de permissão.

Gerenciando usuários tenant e seus privilégios

Não há maneira direta de criar um usuário do tenant. A única maneira de um tenant ter usuários é pela associação com sues unidades de tenant. Os usuários do tenant são todos os usuários em suas próprias unidades de tenants.

A adição de um usuário com uma associação ao acesso a dados do DD Boost ou autoatendimento do tenant usando a CLI pode ser perigosa devido a problemas de tenancy cruzado. A CLI não validará usuários que pertencem a outros tenants ao adicionar usuários com acesso a dados do DD Boost ou usuários de autoatendimento do tenant ao tenant atual.

Você pode criar usuários locais com o DDMC. Se você criar um usuário local com uma função *none* usando o DD System Manager ou a CLI do DDOS, o usuário será exibido na lista de usuários disponíveis do DDMC a serem adicionados ao acesso a dados do DD Boost e/ou ao autoatendimento do grupo de usuários.

Para obter mais informações sobre a criação de um usuário com o DD System Manager, consulte o *DDOS Administration Guide*. Para criar um usuário com a CLI do DDOS, consulte o *DDOS Command Reference Guide*.

Usar o DDMC para administrar o SMT

Para administrar o Secure Multitenancy (SMT) no DDMC, selecione **Administration** > **Multi-tenancy**. O SMT é competível com suporte no DDVE 3.0 e posterior.

Controles

No canto superior esquerdo estão os controles para Adicionar (sinal de + verde), Editar (lápis amarelo) e Excluir (X vermelho) tenants e o ícone Tenant (Unit) Details (i azul) que exibe a lightbox Tenant (Unit) Details (dependendo do que está selecionado). Você também pode clicar com o botão direito do mouse em cada nó na árvore para executar essas funções. O RBAC (Role-Based Access Control, controle de acesso baseado em função) controla todas essas ações.

Árvore de todos os tenants

Abaixo dos controles está a *árvore* de tenants, na qual você pode criar e gerenciar tenants, unidades de tenant e armazenamento provisionado.

O nó All Tenants sempre é exibido e permite a criação de objetos de tenant.

Cada nó possui um controle à sua esquerda, indicando seu status como Warning ou Offline. Esse status acumula nós de tenant e de todos os tenants. Além disso, os controles para a criação, edição ou exclusão de estados são exibidos enquanto cada operação estiver em andamento. Algumas ações podem não ser permitidas, dependendo do estado diferente ou do status dos nós. Se houver unidades de tenant em um tenant com o mesmo nome, um ícone de informação é exibido para o nó de tenant.

O nó Unmanaged é exibido somente se houver unidades de tenant não gerenciadas disponíveis. As únicas ações permitidas no nó Unmanaged e em Unmanaged Tenant Units são *Add all to Tenant* e *Add to Tenant*, respectivamente, e elas estão disponíveis apenas clicando com o botão direito do mouse nos menus de contexto.

O usuário pode clicar em "Unmanaged" e, em seguida, no painel à direita, selecionar todas as unidades de tenant ou unidades de um/vários tenants para adicionar ao tenant. O usuário clica no link "Add to Tenant" para adicionar as unidades de tenant selecionadas ao tenant.

Área Summary

No lado direito há um resumo.

Quando All Tenants for selecionado, o resumo mostra o número total de tenants, unidades de tenant e sistemas host. Você pode ver se algum dos tenants ou unidades de tenant estão off-line ou se estão com problemas de configuração em painéis de severidade diferentes. Também é possível ver o número de unidades de tenant não atribuídas.

Ao selecionar um tenant ou uma unidade de tenant, o resumo inclui (dependendo do item) o nome, status, nome e e-mail do administrador, sistemas host, local do datacenter, alertas e informações de armazenamento e de MTree, usuários do DD Boost, informações de autoatendimento do tenant, agendamento e destinatários de relatório.

Problemas de configuração

Tenants podem ser configurados diretamente nos sistemas Data Domain e PowerProtect. Isso pode levar a conflitos de nome e ID do tenant quando esses sistemas DD forem gerenciados pelo DDMC. O DDMC permite resolver os conflitos de tenant consolidando-os em um único ou separando-os com nomes e IDs exclusivos.

NOTA: Os tenants não podem ser editados ou resolvidos se algum dos sistemas estiverem em estado off-line ou se não puder ser acessado pela rede.

Gerando relatórios, observando a integridade, alterando locais

Para gerar relatórios sobre tenants ou unidades de tenant individuais, selecione **Reports** > **Management**.

Para ver a integridade geral de Tenants e unidades de Tenant, selecione **Health** > **Status**, **Health** > **Alerts** e/ou **Health** > **Jobs**.

Para alterar um local do datacenter, selecione **Administration** > **Properties** e edite a propriedade do datacenter. Cada sistema DD deve ter um valor atribuído explicitamente para o datacenter em **Infrastructure** > **Systems**. Se um sistema tiver uma propriedade de datacenter atribuída, ele será agrupado em *All* no assistente Create Tenant Unit.

Tarefas de administrador de armazenamento no Secure Multitenancy

Os administradores de armazenamento são os *locadores* dos operadores de backup (*tenants*), em um ambiente Secure Multitenancy (SMT). Os administradores de armazenamento instalam e configuram o software e o hardware do sistema e usam o DDMC para provisionar e atribuir armazenamento para os tenants a quem eles dão suporte.

Os administradores de armazenamento em um ambiente SMT executam as seguintes tarefas:

- Migrar usuários de vários sistemas pequenos para um ou mais sistemas maiores
- Isolar os dados de cada tenant de outros tenants que compartilham o armazenamento no mesmo sistema físico
- Monitorar e gerenciar o uso de espaço e desempenho de cada sistema
- Monitorar e gerenciar a utilização de espaço por, e o desempenho fornecido para, cada tenant, o que garante que o administrador de armazenamento atenda aos requisitos do contrato de nível de serviço com cada tenant
- Tenants agrupados com características semelhantes no mesmo sistema físico para obter mais desduplicação cruzada
- Carregar tenants com base em sua utilização de espaço

Tarefas do operador de backup no Secure Multitenancy

Operadores de backup são os *grupos de usuários* em um ambiente do Secure Multitenancy (SMT) Os operadores de backup são responsáveis por agendar e gerenciar backups e replicação para sua organização ou departamento usando o armazenamento disponível em suas unidades de tenant.

Os operadores de backup em um ambiente SMT executam as seguintes tarefas:

- monitorar o desempenho e os recursos de suas unidades de tenant
- monitorar a replicação
- Gerar relatórios

Criar e gerenciar tenants

O DDMC oferece muitas opções para criar e gerenciar tenants.

Criando tenants

Você pode criar Tenants a partir da página Multi-Tenancy.

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Selecione **All Tenants** na árvore e selecione Add Tenant (sinal de mais verde) acima da árvore.
3. Na caixa de diálogo Create Tenant, digite as seguintes informações:
   - Para **Tenant name** [que é obrigatório, conforme indicado pelo asterisco (*)], você pode usar o nome do client ou da organização que utilizará o armazenamento. Por exemplo, se você for um provedor de serviços, o nome pode ser **`XYZ Widget Corp`**. Se você for um administrador de armazenamento de uma organização, o nome pode ser **`Finance Department`**.
   - Para **Administrator name** (que é opcional), digite o nome do administrador de backup.
   - Para **Administrator email** [que é obrigatório, conforme indicado pelo asterisco (*)], digite o endereço de e-mail do administrador de backup. Essas informações serão usadas para criar uma lista padrão Alert Notification.
4. Selecione **Criar**.

Resultados

O novo tenant será exibido na árvore.

Visualizando informações e o status do tenant

Você pode visualizar informações sobre todos os tenants ou tenants individuais na página Multi-tenancy.

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Destaque **All Tenants** para ter uma visão geral dos tenants configurados, de mensagens importantes e do status de geração de relatórios de multi-tenants.
3. Destaque um tenant específico para ver o nome e endereço de e-mail do administrador de backup, mensagens importantes sobre as unidades de tenant para esse tenant e obter informações sobre relatórios dele.
4. Para obter mais detalhes sobre o tenant, selecione Tenant Details (i em azul), acima da lista de tenants, para ver todas as informações disponíveis sobre ele. A *lightbox Tenant Details* está descrita na próxima seção.

Lightbox Tenant Details

A lightbox Tenant Details apresenta informações operacionais detalhadas sobre um tenant específico.

A lightbox de detalhes do tenant é acessada em **Administration** > **Multitenancy**, usando o controle **Tenant Details**.

A página **Overview** possui as seguintes seções:

- **Tenant**, que inclui o nome do tenant, administrador, e-mail do administrador, unidades de tenant e sistemas.
- **Health**, que inclui quatro LEDs para Alerts, File Systems, DD Boost e Replication. Esses alertas podem estar com o estado Normal, Warning ou Error. Você pode passar o mouse sobre um alerta para obter mais informações. A dica de ferramenta sobre os LEDs lista as unidades de tenant que têm problemas, juntamente com um link para iniciar o sistema relacionado a essa unidade de tenant. LEDs de integridade também podem estar em um estado desabilitado se o componente subjacente (ou seja, Replicação, DD Boost e assim por diante) não estiver licenciado ou estiver desabilitado em qualquer um dos sistemas do tenant.
- **Capacity**, que inclui um medidor de capacidade que mostra a utilização atual, valores agregados de cota disponível, cota utilizada, % de cota utilizada (com base em todos os MTrees configurados pertencentes ao tenant) e um banner de aviso/erro, se alguma das cotas não tiver sido habilitada ou configurada.
- **Replication**, que inclui contagens para os pares de replicação automática e sob demanda: total, com erros e com status desconhecido.

- **Network Bytes Used**, que inclui os bytes de replicação total, de backup e de restauração utilizados.

A página **Capacity** mostra os detalhes de Capacity Overview com um medidor de variável que mostra a cota (disponível, utilizada e porcentagem utilizada). O gráfico Logical Space Usage mostra diagramas para pre-comp usados para um tempo selecionado (24 horas, 7 dias, 30 dias, 90 dias ou personalizados, para definir seu próprio período). Há também uma lista de Unidades de tenant associadas a este tenant com seus MTrees ou Unidades de armazenamento, inclusive um painel de severidade com todos os avisos para a unidade de armazenamento/MTree selecionada.

A página **Replication** mostra os detalhes de Replication Overview, que incluem o número total de bytes replicados Para pares de replicação automática e Pares de replicação sob demanda. O gráfico Replication Trend mostra diagramas para pre-comp replicados, post-comp replicados e/ou digramas de taxa de compactação para um tempo selecionado (24 horas, 7 dias, 30 dias, 90 dias ou personalizado, para definir seu próprio período).

A página **Network** mostra os detalhes de Network Overview, que incluem as últimas 24 horas de dados restaurados, de backup e replicação total de entrada e saída. Os gráficos Trend Analysis mostram diagramas para rede total utilizada, bytes de backup e restauração utilizados e bytes de replicação utilizados em um tempo selecionado (24 horas, 7 dias, 30 dias, 90 dias ou personalizado, para definir seu próprio período).

A página **System Charts** mostra os gráficos do sistema para o sistema de uma Unidade de tenant selecionada associada a este tenant. Os gráficos desejados podem ser adicionados à área de gráficos (à direita), habilitando as respectivas caixas de seleção. Você pode exibir gráficos de Recursos para utilização de CPU e throughput de rede; gráficos de File system para Contagens de fluxo, Processamento de protocolo e Throughput de protocolo. Gráficos de replicação para características de entrada/saída e Throughput para cada tipo de replicação. Na área de gráficos, vários gráficos são exibidos verticalmente de acordo com a seleção. Todos esses gráficos podem ser exibidos para um tempo selecionado (24 horas, 7 dias, 30 dias, 90 dias ou personalizado, para definir seu próprio período).

Editando informações do tenant

Você pode alterar os nomes do tenant, nomes do administrador e endereços de e-mail do administrador usando a caixa de diálogo Edit Tenant.

Sobre esta tarefa

Talvez você precise *Resolver conflitos de grupos de usuários* se estiver gerenciando tenants do DDMC e da CLI do DDOS. Os tenants possuem dois identificadores: seu nome e um UUID (Universally Unique ID, ID exclusivo universal). Na CLI do DDOS (Iniciando em 5.7), você pode criar facilmente dois tenants com o mesmo nome, mas UUIDs diferentes. O DDMC detectará isso e se oferecerá para mesclar os dois tenants (fornecendo a eles um UUID recém-criado) ou renomear um dos tenants. Ao concluir, nenhum tenant compartilhará um nome sem também compartilhar uma UUID (e vice-versa).

Se você alterar o nome de um tenant que faz parte de um agendamento de PCM, a alteração do nome não será atualizada automaticamente no agendamento. Você deve adicionar manualmente o novo nome do tenant ao agendamento de PCM.

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Na árvore, selecione o tenant que deseja atualizar e selecione Edit tenant (lápis amarelo) acima da árvore.
3. Na caixa de diálogo Edit Tenant, edite o que precisar e selecione **Save**.

Resultados

O tenant editado será exibido novamente na árvore.

Excluindo tenants

Quando não for mais necessário fornecer armazenamento para uma organização, você pode excluir o tenant que corresponde a essa organização.

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Destaque o tenant na árvore e selecione Delete Tenant (X vermelho) acima da árvore.
3. Na caixa de diálogo Delete Tenant, você tem duas opções:

- **Remove all Tenant Units**, o que preservará os dados para que a unidade de tenant possa ser atribuída a outro tenant. As unidades de tenant serão movidas para o pool da unidade de tenant **Unmanaged** e manterão todas as unidades de armazenamento e todos os MTrees associados a elas.
- **Destroy all Tenant Units**, o que apagará todas as unidades de tenant e quaisquer MTrees e unidades de armazenamento associados a elas.

4. Selecione **Yes**.

NOTA: A exclusão de um tenant não poderá ser *desfeita* a partir do DDMC, por isso tenha muito cuidado ao realizar essa tarefa.

Resultados

O tenant foi excluído da árvore.

O que fazer se a exclusão do tenant falhar

Ao tentar excluir um tenant, a operação poderá falhar por uma série de motivos.

Em primeiro lugar, acesse a página **Health** > **Jobs**, selecione o trabalho com falha e observe o motivo da falha, que pode ser:

- O file system de um ou mais sistemas Data Domain ou PowerProtect no tenant está desativado.
- Alguns dos sistemas Data Domain no tenant não estão acessíveis ou estão desligados.
- O recurso do DD Boost de um ou mais dos sistemas no tenant está desabilitado ou não está licenciado.

Você pode resolver esses problemas manualmente usando o DD System Manager e as interfaces de linha de comando do DDMC (é necessário corrigi-los nos dois locais, pois eles são relacionados ao sistema Data Domain). Em seguida, você pode tentar excluir o tenant novamente usando o DDMC.

Criar e gerenciar unidades do tenant

O DDMC oferece muitas opções para criar e gerenciar unidades de tenant.

Criando uma Unidade de tenant com o assistente

Você pode criar uma unidade de tenant com o Assistente de criação de unidade de tenant.

Pré-requisitos

O armazenamento de um tenant está contido em uma partição virtual chamada *Tenant Unit* em um sistema DD. Para atribuir armazenamento a um tenant, você pode usar o *Assistente de criação de unidade de tenant* para criar a unidade de tenant, provisionar armazenamento e atribuir a unidade dr tenant a um tenant. Também é possível criar uma unidade de tenant vazia para um tenant e provisionar o armazenamento mais tarde.

Selecione **Administration** > **Multitenancy**. Depois, selecione um tenant e o controle **Add** (+ verde).

Durante a criação de uma unidade de tenant, você tem três opções:

- **Create a Tenant Unit with manual provisioning storage**, em que você cria/seleciona os MTrees e Storage Units associados a essa Tenant Unit. Outra opção é criar usuários com acesso a dados do DD Boost para associar às unidades de armazenamento.
- **Create a Tenant Unit with automatic provisioning storage**, em que você pode adicionar usuários com acesso a dados do DD Boost novos ou existentes a essa unidade de tenant. Isso permitirá que o software para backup crie Storage Units que serão atribuídas a essa Tenant Unit.
- **Create an empty Tenant Unit**, em que você pode provisionar a Tenant Unit mais tarde usando a caixa de diálogo Edit Tenant Unit.

Etapas

1. Na primeira página do assistente, identifique o sistema do host:
   - Para **Datacenter location** (que é opcional), selecione um local. Esses locais (por exemplo: Dallas, Nova Iorque) devem ter sido digitados anteriormente como propriedades de localização do datacenter. (**Administration** > **Properties** > **Data Center**)
   - Para **Size now (GiB)** (que é opcional), digite um número para filtrar sistemas que não possuem capacidade suficiente de armazenamento.
   - Para **Size to grow (GiB)** (que é opcional), digite um número para filtrar sistemas que não terão capacidade suficiente em um momento especificado no futuro (definido no próximo campo, "Time to grow"), com base em projeções de capacidade. O tamanho

a aumentar é o tamanho ao qual aumentará no momento especificado. Por exemplo, para um tempo especificado de 6 meses, se o tamanho atual for 1 GiB e o tamanho a aumentar for 2 GiB, em 6 meses, o requisito mínimo de capacidade seria 2 GiB.

- Para **Time to grow** (que é opcional), digite o tempo após o qual o volume de capacidade de "Size to grow" deve ser atingido.

2. Na segunda página do assistente, Select Host System, você verá os sistemas que possuem capacidade lógica suficiente para hospedar a Tenant Unit:

   Como verificar o desempenho do sistema do host? Use as informações a seguir para determinar o melhor sistema no qual deseja criar a unidade de tenant.

   - **Available now** indica os sistemas que você pode selecionar agora.
   - **Available in 6 months** é exibido se você selecionou 6 meses no campo "Time to grow" na página anterior ou se não selecionou um valor explicitamente. **Available in 12 months**, **Available in 18 months** ou **Available in 24 months** são exibidos se você tiver selecionado esses valores em "Tempo a aumentar". Por exemplo, para um tempo especificado de 6 meses, se o tamanho atual for 1 GiB e o tamanho a aumentar for 2 GiB, em 6 meses, o requisito mínimo de capacidade seria 2 GiB. Qualquer sistema que tenha uma menor capacidade projetada será filtrado na lista. Além disso, qualquer sistema off-line no momento, bem como qualquer sistema de destino de coleta, será filtrado na lista. Somente os sistemas que executam DDOS 5.6 ou posterior são listados.
   - **Existing Tenant Units** exibe o número atual de unidades de tenant no sistema.
   - Para sistemas com um controle de informações (*i* azul), você pode passar o mouse para ver uma mensagem de advertência explicando por que uma projeção não pode ser feita.
   - Se um sistema não estiver listado, talvez seja porque ele:
     - não se encontra no datacenter especificado.
     - está off-line.
     - está executando o DDOS 5.6 ou anterior.
     - não tem capacidade suficiente.
     - possui um destino de replicação.
     - é um sistema para o qual você não tem privilégios administrativos.
   - Para o sistema selecionado, os gráficos na parte inferior exibem dados históricos, que incluem **Throughput** para a porta de conexão selecionada, utilização de **CPU** de cada sistema e **Stream Count**. Você pode mudar dos menus drop-down da porta e tempo (últimos 7 dias, últimos 30 dias ou últimos 90 dias) para obter diferentes conjuntos de dados.

3. Na terceira página do assistente, Administration, digite o nome e os detalhes do administrador:
   - Para **Tenant Unit name** [que é obrigatório, conforme indicado com o asterisco (*)], digite um nome exclusivo de Tenant Unit por sistema.
   - Para **Administrator name** (que é opcional), digite o nome do administrador de backup.
   - Para **Administrator email** [que é obrigatório, conforme indicado com o asterisco (*)], digite o endereço de e-mail do administrador de backup. Isso será usado para criar uma lista padrão Alert Notification.
   - Quando **Create an Empty Tenant Unit** for selecionado, a opção **Use strict security mode** não será exibida.
   - Selecione **Use strict security mode** se desejar permitir futuras replicações somente se forem provenientes de outra Tenant Unit que pertença ao mesmo tenant.
   - Selecione ou digite **Management IP Addresses** (que é opcional), conforme necessário.

   NOTA: Consulte a seção a seguir, Modo de segurança e endereços IP de gerenciamento na página 75, para obter mais informações sobre esses tópicos.

4. A quarta página do assistente depende da escolha anterior. [Observe que para "Create an empty Tenant Unit", você vai para a página final (etapa 5).]

   a. Para o provisionamento manual, você pode criar unidades de armazenamento/MTrees.
      - As unidades de armazenamento/MTrees podem ser adicionadas aqui, durante a criação de uma unidade de tenant com Provisionamento manual. Você também pode adicioná-las ao editar uma unidade de tenant.
      - É possível adicionar novos MTrees ou unidades de armazenamento ou selecionar entre os MTrees ou unidades de armazenamento já existentes no sistema do host.
      - Você também pode editar, cancelar a atribuição ou destruir MTrees ou unidades de armazenamento na mesma área.
      - Se a seleção de um MTree ou unidade de armazenamento não for permitida, você poderá passar o mouse sobre ela para obter mais informações.

   b. Para o provisionamento automático, você pode configurar os usuários para acesso a dados por meio do protocolo DD Boost.
      - Você pode adicionar um usuário local existente ou criar um novo usuário local e promover o usuário local a usuário do DD Boost.
      - Você pode excluir o usuário do DD Boost selecionado.
      - A tabela contém nomes de usuário com acesso a dados do DD Boost e a contagem de unidades de armazenamento associadas ao usuário.
      - O painel de informações mostra quando um ou mais usuários estão selecionados.
      - A configuração não é alterada até que você selecione Create na página Summary.

- Se houver um ou mais usuários locais na lista, o primeiro usuário local da lista será selecionado por padrão. Se não houver nenhum usuário local na lista, "New local user" será selecionado. Todos os usuários selecionados ou usuários recém-criados serão automaticamente unidades de tenant padrão.
- Um aviso será exibido se o usuário local selecionado atualmente já tiver outra Tenant Unit como sua Tenant Unit padrão.
- A primeira entrada na lista drop-down "Local user" é "New local user", que permite que você crie um novo usuário local e adicione-o como um usuário com acesso a dados do DD Boost.
- Ao selecionar "New local user", a caixa de diálogo Add Data Access User é alterada para um formulário **Add New Data Access User**.

5. A quinta página (final) (quarta página para "Create an empty Tenant Unit") do assistente é um Resumo que mostra os dados das páginas anteriores.
   - A unidade de tenant não será criada até que você selecione Create.
   - Você tem a opção de enviar um e-mail para o administrador da unidade de tenant sobre a criação bem-sucedida da mesma.
   - A criação de uma Tenant Unit com qualquer tipo de provisionamento (não vazia) gera automaticamente um par de Modelos de relatórios (Status e Utilização) e os agenda.
   - Você pode receber um dos dois avisos: (1) você não provisionou essa unidade de Tenant corretamente. Adicione MTrees ou armazenamento. (2) Você não provisionou essa unidade de tenant corretamente. Torne essa unidade de tenant a unidade padrão para um dos Usuários com Acesso de Dados do DD Boost.

Resultados

A unidade de tenant criada recentemente será adicionada à árvore.

O que fazer se a criação da unidade de tenant falhar

A criação de uma unidade de tenant pode falhar por vários motivos.

Ela pode falhar por motivos simples, como um nome duplicado da Tenant Unit ou pode falhar se houver alterações repentinas do estado do sistema, como um problema de rede/conectividade.

No processo de criação em si, pode haver falhas onde MTrees ou unidades de armazenamento podem falhar por um ou mais motivos ao serem criados ou os usuários do DD Boost podem não ser criados.

A criação de uma unidade de tenant será bem-sucedida mesmo se a configuração de um componente individual, como MTrees ou usuários do DD Boost, falhar. Portanto, os componentes finais de uma Tenant Unit recém-criada podem não corresponder às especificações.

Para ver as informações de sucesso e/ou falha para cada tarefa, ou se há uma inconsistência entre o que era esperado e o que foi criado, selecione **Health** > **Jobs** para ver mensagens adicionais.

Você deve resolver os motivos da falha antes de tentar recriar uma nova unidade de tenant ou correrá o risco de ver as mesmas situações de falha novamente.

Modo de segurança e endereços IP de gerenciamento

Strict Security Mode garante que a replicação de entrada seja de outra unidade de tenant pertencente ao mesmo tenant. Além disso, esse modo deve ser habilitado para permitir conexões de gerenciamento para ou de IPs atribuídos. *Management IP addresses* permite associar uma unidade de tenant a certos endereços IP para clients remotos e outros sistemas locais do DDMC.

Sobre esta tarefa

- *Remote client addresses* são endereços IP dos quais as conexões de entrada serão aceitas. Esses endereços devem ser IPv4 ou IPv6.
- *Local DDMC addresses* são endereços IP disponíveis para gerenciar e conectar a essa unidade de tenant. Você pode digitar novos endereços que serão configurados no sistema Data Domain. Ou pode selecionar entre endereços IPv4 ou IPv6 configurados no sistema Data Domain que não estejam atribuídos a outras unidades de tenant. (Os endereços IP atribuídos ficam indisponíveis e não podem ser selecionados).

Visualizando informações e o status da unidade de tenant

Você pode visualizar informações sobre todas as unidades de tenant na página Multitenancy.

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Selecione uma unidade de tenant na árvore para exibir uma página de resumo e os alertas críticos.

3. Para obter mais detalhes sobre a unidade de tenant, selecione Tenant Unit Details (o i azul), sobre a árvore, para ver todas as informações disponíveis sobre a unidade de tenant. A *lightbox Tenant Unit Details* está descrita na próxima seção.

Lightbox Tenant Unit Details

A lightbox Tenant Unit Details apresenta informações operacionais detalhadas sobre uma unidade de tenant específica.

A lightbox Tenant Unit Details pode ser acessada na página **Administration** > **Multitenancy**, **Health** > **Status** ou **Health** > **Alerts** (visualização Tenants), usando o controle **TENANT UNIT DETAILS**.

A página **Overview** possui as seguintes seções:

- **Tenant Unit**, que inclui nome do tenant ou da unidade de tenant, administrador, e-mail do administrador, sistema de host e local do data center.
- **Health**, que inclui quatro LEDs para Alerts, File Systems, DD Boost e Replication. Esses alertas podem estar com o estado Normal, Warning ou Error. Você pode passar o mouse sobre um alerta para obter mais informações. LEDs de integridade também podem estar em um estado desabilitado se o componente subjacente (ou seja, Replicação, DD Boost e assim por diante) não estiver licenciado ou estiver desabilitado para o sistema da Unidade de tenant selecionada.
- **Host System Performance Details**, que mostra o fluxo de dados para Throughput, CPU e Contagem de fluxo. Portas de rede diferentes podem ser selecionadas. As durações do gráfico podem ser selecionadas entre: últimas 24 horas, 7 dias, 30 dias, 90 dias e personalizados.
- **Capacity**, que inclui um medidor de capacidade que mostra a utilização atual, valores agregados de cota disponível, cota utilizada, % de cota utilizada (com base em todos os MTrees configurados pertencentes à unidade de tenant) e um banner de aviso/erro, se alguma das cotas não tiver sido habilitada ou configurada.
- **Replication**, que inclui contagens (entradas e saídas) para os pares de replicação automática e sob demanda: total, com erros e com status desconhecido.
- **Network Bytes Used**, que inclui os bytes de replicação total, de backup e de restauração utilizados.

A página **Capacity** mostra os detalhes da Capacity Overview com um medidor de variável que mostra a porcentagem de cota utilizada; um gráfico de Logical Space Usage, que pode ser dimensionado para visualizar determinados períodos de utilização; e uma lista de unidades de tenant com seus MTrees ou unidades de armazenamento, inclusive um painel de severidade com todos os avisos para a unidade de armazenamento/MTree selecionada.

A página **Replication** mostra os detalhes de Replication Overview, que incluem o número total de bytes replicados Para pares de replicação automática e Pares de replicação sob demanda. O gráfico Replication Trend mostra pelo menos um dos mesmos, os diagramas de taxa de compactação replicada e de compactação do post-comp replicados em um gráfico de tempo personalizado.

A página **Network** mostra os detalhes de Network Overview, que incluem as últimas 24 horas de dados restaurados, de backup e replicação total de entrada e saída. A análise de tendências mostra gráficos que podem ser visualizados por um determinado período, selecionando uma das quatro opções (24 horas, 7 dias, 30 dias, 90 dias) ou selecionando Personalizado, o que permite selecionar um intervalo de tempo diferente.

A página **System Charts** mostra os gráficos do sistema para o sistema da unidade de tenant selecionada. Os gráficos desejados podem ser adicionados à área de gráficos (à direita), habilitando as respectivas caixas de seleção. Você pode exibir gráficos de Recursos para a utilização da CPU e o Throughput da rede. Gráficos de file system para Contagens de fluxo, Processamento de protocolo e Throughput de protocolo; Gráficos de replicação para características de entrada/saída e Throughput para cada tipo de replicação. Na área de gráficos, vários gráficos são exibidos verticalmente de acordo com a seleção.

Editando informações da unidade de tenant

Você pode alterar todos os tipos de informações de unidades de tenant gerenciadas e não gerenciadas usando a caixa de diálogo Edit Tenant Unit.

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Selecione a unidade de tenant na árvore e selecione Edit Tenant Unit (lápis amarelo) acima da árvore.
3. A caixa de diálogo Edit Tenant Unit tem as seguintes guias: General, Alert Notifications, DDBoost Streams, MTrees, Data Access Users e Tenant Self-Service que são descritas nas seções a seguir.

Editar unidades de Tenant: guia geral

Você pode alterar informações administrativas de unidades de tenant gerenciadas e não gerenciadas usando a guia General na caixa de diálogo Edit Tenant Unit.

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Selecione uma unidade de tenant na árvore e selecione Edit Tenant Unit (lápis amarelo) acima da árvore.
3. Na guia General, você pode alterar o seguinte:
   - Nome da unidade de tenant
   - Nome do administrador
   - E-mail do administrador — se o e-mail do administrador for modificado, os modelos de relatório que enviam relatórios associados à unidade de tenant para este administrador precisarão ser redirecionados. Após editar o e-mail do administrador, um pop-up será exibido confirmando se uma alteração precisa ser feita em todos os modelos de relatório associados ao e-mail antigo. Se você selecionar Yes, todos os e-mails antigos do administrador serão substituídos pelo novo valor.
   - Modo de segurança — Você pode optar por habilitar o *modo estrito de segurança*, que garante que qualquer replicação de entrada seja de outra unidade de tenant pertencente ao mesmo tenant. Além disso, esse modo deve ser habilitado para permitir conexões de gerenciamento para ou de IPs atribuídos.
   - Endereços IP de gerenciamento — Você pode adicionar ou excluir endereços IP de gerenciamento para endereços de clients remotos ou endereços locais do DDMC.

Editar unidades de Tenant: guia Alert Notifications

Cada unidade de tenant possui uma lista de notificações de alertas padrão (criada pelo sistema Data Domain ou PowerProtect) que contém o e-mail do administrador. Você pode criar listas de notificações de alertas, editar listas existentes ou excluir listas associadas à unidade de tenant, usando a guia Alert Notifications na caixa de diálogo Edit Tenant Unit.

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Selecione uma unidade de tenant na árvore e selecione Edit Tenant Unit (lápis amarelo) acima da árvore.
3. Na guia Alert Notifications, selecione Add (sinal de mais verde).
4. Na caixa de diálogo Add Alert Notification Group, digite um nome para o grupo de notificação.
5. Selecione Add (sinal de mais verde) e digite o primeiro endereço de e-mail.

   Você pode continuar selecionando Add para digitar mais endereços.
6. Selecione **ADD** na parte inferior da caixa de diálogo quando terminar de adicionar endereços e, em seguida, selecione **SAVE** para salvar suas alterações.

Editando unidades de tenant: guia Data Access Users

Data Access Users são aqueles que estão configurados para unidades de tenant específicas (um ou mais usuários por unidade de tenant). Opcionalmente, você pode designar uma unidade de tenant como a unidade de armazenamento padrão para um usuário com acesso a dados. Quando o software de backup cria unidades de armazenamento para um usuário, o software usa automaticamente a unidade de tenant padrão.

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Selecione uma unidade de tenant na árvore e selecione Edit Tenant Unit (lápis amarelo) acima da árvore.
3. Na guia Data Access Users, adicione, edite ou exclua usuários. Novos usuários com acesso a dados recebem a função de none. Se um usuário já tiver sido criado com uma função diferente de none, esse usuário é desativado e somente poderá ser excluído da tabela. Além disso, se um usuário já tiver sido associado a vários tenants, esse usuário é desativado e somente poderá ser excluído da tabela. A validação da senha de um novo usuário local é baseada na força da política de senha do DD OS associada à unidade de tenant atual.
4. As colunas indicam:
   - **MTrees Accessed** — o total combinado de unidades de armazenamento e pools do vDisk.

- **MTree Type** — os tipos compatíveis são a unidade de armazenamento e pool do vDisk. Se um usuário não estiver associado ao acesso de um MTree, o tipo de MTree será None.

5. Clique em **SAVE** para salvar as alterações.

Corrigindo um problema de Double Agent

Usuários *Double Agent* com acesso a dados são usuários associados a mais de um tenant.

Sobre esta tarefa

Se um usuário local possuir várias unidades de armazenamento e as unidades de tenant que contêm essas unidades de armazenamento não pertencerem todas ao mesmo tenant, isso é definitivamente uma desconfiguração e sempre resultará em uma violação de segurança (o isolamento administrativo ou de dados é violado). Essa situação também pode resultar em erros no relatório de utilização do tenant.

Os efeitos da desconfiguração dependem de quais tenants realmente possuem os dados nas unidades de armazenamento afetadas. Se os dados em todas essas unidades de armazenamento na verdade pertencerem a um único tenant, não há nenhuma violação de segurança do isolamento de dados (cada tenant pode acessar apenas seus próprios dados), mas os relatórios de utilização para os tenants estarão incorretos. Alguns tenants visualizarão a utilização das unidades de armazenamento que pertencem a outros tenants, enquanto alguns tenants não visualizarão a utilização de algumas de suas unidades de armazenamento. Além disso, alguns tenants poderão visualizar os nomes e a utilização das unidades de armazenamento do outro tenant. Isso também é uma violação de segurança do isolamento administrativo.

Se algumas unidades de armazenamento contiverem os dados de um tenant e outras unidades de armazenamento contiverem os dados de um tenant diferente, diferentes tenants receberam as mesmas credenciais do usuário para acessar suas unidades de armazenamento, portanto, há uma violação de segurança do isolamento de dados, já que cada tenant pode acessar os dados do outro tenant nas unidades de armazenamento pertencentes ao usuário local compartilhado. No entanto, os relatórios de utilização para cada tenant estarão corretos nesse caso.

Corrigindo um problema de usuário que não seja "none"

Os usuários com acesso a dados sempre devem ter a função *none*.

Sobre esta tarefa

Um usuário que não tem função de *none* já está associado a um tenant. Portanto, as credenciais do usuário (usuário/senha) de um usuário que tem permissão para visualizar e possivelmente até mesmo alterar a configuração/os dados no sistema foram dadas a um Tenant. Se o usuário tiver a função de *admin*, por exemplo, o tenant pode agora acessar (ler/gravar) os dados de qualquer outro tenant e exibir/alterar qualquer configuração do sistema.

Essa violação de segurança estará presente esteja esse usuário (com função não *none*) associado a apenas um tenant ou a múltiplos e diferentes tenants. A principal violação de segurança não é que um usuário seja usado por vários tenants, mas que um usuário concedido a um tenant para utilização possa visualizar e/ou modificar a configuração e os dados que não pertencem ao tenant.

Para impedir violações de segurança, os usuários com acesso a dados devem *sempre* ter uma função de *none*. Em algumas configurações do cliente, em que os tenants são considerados confiáveis, eles podem ter alguns usuários com função não *none*, mas a prática recomendada de segurança é não permitir isso.

Corrigindo um problema de usuário que não seja "none" e de Double Agent

Às vezes, pode haver casos em que um usuário com acesso a dados *tanto* não tem a função *none* como também é um usuário *Double Agent*, que é um usuário associado a mais de um tenant. Você deve resolver esses dois problemas antes de continuar.

Sobre esta tarefa

Um usuário que não tem função de *none* já está associado a um tenant. Portanto, as credenciais do usuário (usuário/senha) de um usuário que tem permissão para visualizar e possivelmente até mesmo alterar a configuração/os dados no sistema foram dadas a um Tenant. Se o usuário tiver a função de *admin*, por exemplo, o tenant pode agora acessar (ler/gravar) os dados de qualquer outro tenant e exibir/alterar qualquer configuração do sistema. (Consulte a seção anterior, Corrigindo um problema de usuário que não seja "none" na página 78, para obter mais informações sobre esse problema.)

O usuário *Double Agent* pode ter várias unidades de armazenamento, mas as unidades de tenant que contêm essas unidades de armazenamento não pertencem todas ao mesmo tenant, isso é definitivamente uma desconfiguração e sempre resulta em uma violação de segurança (os dados ou isolamento administrativo são violados). Essa situação também pode resultar em erros no relatório de utilização

lo tenant. (Consulte a seção anterior, Corrigindo um problema de Double Agent na página 78, para obter mais informações sobre esse problema.)

Editando unidades de tenant: Guia DD Boost Streams

Você pode limitar o número de fluxos que um aplicativo pode usar ao ler ou gravar dados em uma unidade de armazenamento. Se um client utilizar mais do que o limite definido, um alerta será gerado pelo sistema Data Domain.

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Destaque uma unidade de tenant na árvore e selecione Edit Tenant Unit (lápis amarelo) acima da árvore.
3. Na guia DD Boost Streams, visualize as unidades de armazenamento associadas a essa unidade de tenant.
4. Se desejar definir os limites para uma unidade de armazenamento, selecione essa unidade e, em seguida, **Set Limits**.

Configurando limites de fluxo do DD Boost

Você pode configurar limites de advertência de fluxo para cada unidade de armazenamento para quatro itens: Read, Write, Replication e Combined. Quando qualquer uma dessas contagens de fluxo exceder o limite de advertência, um alerta será gerado.

Etapas

1. Selecione **Set Limits** na guia **DDBoost Streams** da caixa de diálogo **Edit Tenant Unit** [que você pode obter selecionando **Administration** > **Multi-Tenancy** e, em seguida, selecionando uma unidade de tenant e Edit Tenant Unit (lápis amarelo)].
2. Na caixa de diálogo Set DDBoost Stream Limits, digite valores para os limites de fluxo de Read, Write, Replication e Combined. Não exceda os limites do sistema DD. Observe também que um único valor não pode ser maior que o limite combinado.

   Para limites fixos, há duas outras regras de validação:
   - O limite combinado também não é maior do que a soma dos outros limites fixos (se for, um dos outros limites será atingido primeiro e nunca o limite combinado).
   - O limite combinado é menor do que o limite fixo individual máximo (se for, esse limite individual nunca será atingido, ou seja, o limite combinado sempre será atingido primeiro).
3. Se os limites forem ultrapassados, um alerta será gerado pelo sistema.
4. Selecione Set.

Editando unidades de tenant: Guia MTrees

Você pode criar e gerenciar MTrees, unidades de armazenamento, Pools do vDisk e Pools de VTL usando a guia MTrees na caixa de diálogo Edit Tenant Unit. Além desse método, também é possível adicioná-los quando estiver criando uma unidade de tenant com provisionamento manual.

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Destaque uma unidade de tenant na árvore e selecione Edit Tenant Unit (lápis amarelo) acima de árvore.
3. Na guia MTrees, adicione, edite ou exclua MTrees, unidades de armazenamento, Pools do vDisk e Pools de VTL, conforme desejado.

   NOTA: vDisks com usuários *Double Agent* com acesso a dados (ou seja, usuários associados a outro tenant) ou usuários com uma função diferente de *none* não podem ser associados à unidade de tenant.
4. Se a cota de capacidade estiver habilitada no sistema host, é possível editar cotas flexíveis e fixas.

Ajustando cotas flexíveis/fixas de MTrees e unidades de armazenamento

As cotas podem ser habilitadas ou desabilitadas em um sistema de host usando a interface de linha de comando (CLI) ou com o DD System Manager. Você não pode habilitar ou desabilitar cotas usando o DDMC. Você pode *ajustar* cotas usando o DDMC se as cotas do sistema de host já tiverem sido habilitadas.

Pré-requisitos

As cotas do sistema de host já devem estar habilitadas.

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Marque a unidade de tenant na árvore e selecione Edit Tenant Unit (lápis amarelo) acima da árvore.
3. Na guia MTrees, destaque uma unidade de armazenamento ou MTree na lista e selecione Editar (lápis amarelo).
4. Defina os valores de cota desejados na caixa de diálogo Edit MTree ou Edit Storage Unit e selecione **ADD**.
5. Clique em **SAVE** para salvar as alterações.

Próximas etapas

Você também pode habilitar ou desabilitar cotas no sistema de host da seguinte maneira:

1. Inicie o DD System Manager, para o sistema Data Domain ou PowerProtect específico no DDMC.
2. Selecione **Data Management** > **Quota tab**.
3. Habilite ou desabilite cotas, conforme necessário.

Você também pode habilitar ou desabilitar cotas usando a CLI. Consulte o *DD OS Command Reference Guide*.

Editar unidades de Tenant: guia Tenant Self-Service

O *Autoatendimento de tenant* é um método de permitir que um tenant faça log-in em um sistema Data Domain ou PowerProtect para realizar alguns serviços básicos (adicionar, editar ou excluir usuários locais, grupos de NIS e/ou grupos do AD). Isso reduz o gargalo de sempre ter de passar por um administrador para essas tarefas básicas. O tenant pode acessar somente suas unidades de tenant atribuídas. Observe que usuários de tenant e administradores de tenant possuem privilégios diferentes.

Sobre esta tarefa

Para criar uma lista de usuários que podem ter acesso de autoatendimento a uma unidade de tenant específica:

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Selecione uma unidade de tenant na árvore e selecione Edit Tenant Unit (lápis amarelo) acima da árvore.
3. Na guia Tenant Self-Service, você deve primeiro ativar o Tenant Self-Service. (Desativado por padrão).
4. nesta tabela:
   - A coluna **Type** exibe o usuário de gerenciamento ou grupo de gerenciamento.
   - A coluna **Group Type** exibe NIS ou Active Directory para grupos e N/A para usuários.
   - A coluna **Role** exibe administrador de tenant ou usuário de tenant.
5. Para adicionar um usuário de autoatendimento, selecione Add (sinal de mais verde). Na caixa de diálogo Add Self-Service User, selecione o usuário local desejado, grupo do NIS ou grupo do AD, ou crie um novo usuário local (não há nenhum padrão). Se você selecionar New local user, a caixa de diálogo adicionará campos para Name, Password/Confirm e Role (tenant-admin ou tenant-user). A validação da senha de um novo usuário local é baseada na força da política de senha do DD OS associada à unidade de tenant atual.
6. Para editar um usuário de autoatendimento, selecione um usuário ou grupo e selecione Edit (lápis amarelo). Você pode alterar a função de tenant-admin para tenant-user ou vice-versa.
7. Para excluir um usuário de autoatendimento, selecione um usuário ou grupo e selecione Delete (X). Uma caixa de diálogo de confirmação é exibida para assegurar que você realmente deseja excluir este usuário ou grupo. Um novo usuário ou grupo de autoatendimento de tenant será atribuído à função de *none*. Se um usuário ou grupo já tiver sido criado com uma função diferente de *none*, esse usuário ou grupo será desativado e só poderá ser excluído da tabela. Além disso, se um usuário ou grupo já tiver sido associado a vários tenants, esse usuário ou grupo será desativado e só poderá ser excluído da tabela.

Excluindo unidades de tenant e cancelando a atribuição de armazenamento provisionado

Você pode excluir unidades de tenant e, caso uma delas tenha armazenamento provisionado, você pode cancelar a atribuição desse armazenamento para ser reatribuído posteriormente a outra unidade de tenant ou pode destruir todos os dados. *Tenha muito cuidado* ao executar essa tarefa, pois ela não pode ser desfeita.

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Selecione uma unidade de tenant na árvore e selecione Delete Tenant Unit (X vermelho) acima da árvore.
3. Na caixa de diálogo Delete Tenant Unit, se a unidade de tenant tiver armazenamento aprovisionado, você terá duas opções:
   - **Unassign all storage**, que mantém todos os MTrees e unidades de armazenamento associados à unidade de tenant para que possam ser reatribuídos posteriormente para outra unidade de tenant.
   - **Destroy all storage**, que exclui todos os MTrees e unidades de armazenamento associados à unidade de tenant.
4. Selecione **YES** para excluir a unidade de tenant.
5. Observe que a unidade de tenant foi excluída da árvore.

   O que fazer se a exclusão da unidade de tenant apresentar falha

   Ao tentar excluir uma unidade de tenant, a operação poderá falhar por diversos motivos.

   Em primeiro lugar, acesse a página **Health** > **Jobs**, selecione o trabalho com falha e observe o motivo da falha, que pode ser:

   - O file system do sistema no qual reside a unidade de tenant está desativado.
   - O sistema DD em que a unidade de tenant reside não está acessível ou está desligado.
   - O recurso do DD Boost do sistema no qual a unidade de tenant reside está desabilitado ou não está licenciado.

   Você pode resolver esses problemas manualmente usando o DD System Manager e as interfaces de linha de comando do DDMC (é necessário corrigi-los nos dois locais, pois eles são relacionados ao sistema). Em seguida, você pode tentar excluir a unidade de tenant novamente usando o DDMC.

Adicionando uma unidade não gerenciada de tenant a um tenant

Ao trabalhar na CLI (command-line interface, interface de linha de comando) do DD OS, os administradores podem criar unidades de tenant sem adicioná-las a tenants. Essas unidades de tenant são chamadas de *não gerenciados*. No DDMC, não é possível criar uma unidade de tenant não gerenciada, mas é possível adicionar uma unidade de tenant não gerenciada a um tenant.

Etapas

1. Selecione **Administration** > **Multitenancy**.
2. Selecione o nó Unmanaged na árvore. Uma tabela será exibida à direita, a qual contém todas as unidades de tenant não gerenciadas e os sistemas host nos quais elas residem.
3. Para adicionar todas as unidades de tenant não gerenciadas a um tenant, clique com o botão direito no nó Unmanaged e selecione Add all to Tenant. Na caixa de diálogo Add (All) Tenant Units, selecione o nome do tenant e, depois, Add.
4. Se quiser adicionar apenas uma unidade ou mais unidades específica(s) de tenant a um tenant, volte à tabela para selecionar a(s) caixa(s) de seleção ao lado das unidades. Ou, para selecionar uma única unidade de tenant e ver um resumo sobre ela, é possível expandir a lista **Unmanaged** (se já não estiver expandida) e selecionar uma única unidade de tenant.
5. No canto superior direito, selecione o link **Add to Tenant**.
6. Na caixa de diálogo Add Tenant Unit(s), selecione um nome do tenant e depois **Add**. A unidade de tenant será movida do nó não gerenciado para o tenant selecionado, na árvore.

Próximas etapas

Você pode identificar um possível conflito ao tentar atribuir uma unidade de tenant.

Suponha que você tem um usuário do DD Boost ou usuário de autoatendimento do tenant configurado em uma unidade de tenant atual não gerenciada. Se o mesmo usuário estiver configurado para a unidade de tenant gerenciada do Tenant T2, mas você deseja atribuir a unidade de tenant ao Tenant T1, isso é considerado um conflito e não é permitido.

Criando, editando e gerando relatórios do SMT

Você pode criar, editar e gerar relatórios para o Secure Multi-Tenancy (SMT) usando o DDMC.

Tabela de permissão de relatório do SMT

As permissões para trabalhar com a criação e visualização de relatórios de tenants e unidades de tenant dependem da função do usuário no DDMC e no DD OS.

Tabela 13. Tabela de permissão para Tenants e unidades de Tenant, administrador e administrador limitado do DDMC

Função de usuário do DDMC/DD OS	Administrador do DDMC/sysadmin do DD OS	Administrador limitado do DDMC/sysadmin do DD OS
Modelo de relatório		
Exibir todos os modelos de relatório	yes	yes
Visualizar informações sobre configuração do relatório de tenant na página de resumo	yes	yes
Visualizar informações sobre configuração do relatório da unidade de tenant na página de resumo	yes	yes
Criar modelo automático de relatório de tenant	yes	yes
Criar modelo automático de relatório de unidade de tenant	yes	yes
Criar modelo manual de relatório de tenant	yes	yes
Criar um modelo manual de relatório de unidade de tenant	yes	yes
Manter e marcar a configuração do modelo de relatório do SMT	yes	yes
Excluir/destruir relatórios relacionados ao MTree	yes	não

Tabela 14. Tabela de permissão para tenants e unidades de tenant, usuário do DDMC

Função de usuário do DDMC/DD OS	Usuário do DDMC/sysadmin do DD OS	Usuário do DDMC/usuário ou operador de backup do DD OS	Usuário do DDMC/nenhuma função do DD OS
Modelo de relatório			
Exibir todos os modelos de relatório[2]	não	não	não
Visualizar informações sobre configuração do relatório de tenant na página de resumo[2]	não	não	não
Visualizar informações sobre configuração do relatório da unidade de tenant na página de resumo	yes	yes	não
Criar modelo automático de relatório de tenant	não	não	não

Tabela 14. Tabela de permissão para tenants e unidades de tenant, usuário do DDMC (continuação)

Função de usuário do DDMC/DD OS	Usuário do DDMC/sysadmin do DD OS	Usuário do DDMC/usuário ou operador de backup do DD OS	Usuário do DDMC/nenhuma função do DD OS
Criar modelo automático de relatório de unidade de tenant	yes	yes	não
Criar modelo manual de relatório de tenant[c]	não	não	não
Criar um modelo manual de relatório de unidade de tenant	yes	yes	não
Manter e marcar a configuração do modelo de relatório do SMT[d]	yes	yes	não
Excluir/destruir relatórios relacionados ao MTree	não	não	não

a. O usuário do DDMC pode visualizar apenas os modelos ou relatórios criados por ele.
b. Somente o *admin* do DDMC deve ter permissão para criar o modelo de relatório de tenant.
c. O usuário do DDMC não tem permissão para criar manualmente um modelo de relatório de tenant.
d. Se os relatórios de um usuário do DDMC forem excluídos, o usuário será avisado e os relatórios serão criados novamente e marcados somente para esse usuário.

Criando modelos de relatório de SMT

Os modelos de relatório de SMT (Secure Multi-Tenancy) configuram o status diário e as métricas de utilização de Tenants e Tenant Units.

Sobre esta tarefa

NOTA: Se um usuário que é o "proprietário" de qualquer modelo de relatório for excluído do DDMC, esses modelos de relatório serão atribuídos a um novo proprietário ou excluídos. Se esses modelos forem atribuídos a um novo proprietário, os relatórios não serão mais executados nos períodos agendados.

Etapas

1. Selecione **Reports** > **Management**.
2. Selecione Add (sinal de mais verde).
3. Na caixa de diálogo Add Report Template, selecione **Multitenancy Reports** e depois **Next**.
4. Digite um nome e selecione um modelo. As opções de modelo são **Daily Status** ou **Usage Metrics**. Escolha uma ou mais seções para incluir e selecione **Next**.
5. Selecione um escopo (**Tenant Unit** ou **Tenant**). O relatório Daily Status está sempre configurado para mostrar as últimas 24 horas de dados históricos e você pode selecionar a retenção do relatório (sempre, 7 dias, 30 dias, 90 dias). O relatório Usage Metrics (que é gerado como uma planilha do Excel) permite que você exiba dados para um mês completo ou uma semana completa. Selecione **Edit** para definir um agendamento para a frequência e a hora em que o relatório é executado. A hora de geração do relatório será duas horas após a hora *Starts On*.
6. Para o modelo de relatório de Tenant Unit, as mensagens de e-mail do administrador de Tenant Unit são adicionadas por padrão. Para o modelo de relatório de tenant, o e-mail do administrador de tenant é adicionado por padrão. Você pode adicionar ou remover manualmente essas mensagens de e-mail.
7. Analise os detalhes e selecione para salvar o modelo para uso posterior e/ou para executar o relatório imediatamente. Selecione **Finish.**

Resultados

Depois de ter sido criado, um modelo de relatório Multi-Tenancy é adicionado como uma entrada na tabela de relatórios. Quando selecionado, o modelo pode ser usado para executar imediatamente um relatório, pode ser editado ou excluído, ou a hora em que foi executado pela última vez pode ser exibida.

Editando modelos de relatório do SMT

Você pode reconfigurar um modelo de relatório do SMT usando o controle Edit. O conteúdo do relatório, o agendamento e a distribuição de e-mails podem ser modificados no modelo.

Etapas

1. Selecione **Reports** > **Management**.
2. Selecione um modelo e selecione Edit (lápis amarelo). Na caixa de diálogo Edit Report, você pode selecionar uma das quatro guias.
3. Na guia **CONTENT**, o nome do modelo pode ser renomeado e as seções de modelo podem ser selecionadas novamente para o relatório. O modelo, em si, não é editável.
4. Nas guias **SCOPE** e **SCHEDULE**, o escopo do modelo e o agendamento podem ser alterados. O modelo de relatório pode ser alterado de um relatório de tenant para um relatório de unidade de tenant ou de um relatório de unidade de tenant para um relatório de tenant. Para o modelo de relatório de status diários, o agendamento pode ser alterado somente para hora diária. Para o modelo de relatório de utilização, o intervalo de tempo pode ser semanal ou mensal. Se o intervalo de tempo for semanal, apenas semanal pode ser agendado para a hora *start on* e se o intervalo de tempo for mensal, apenas mensal pode ser agendado para a hora *start on*. O status diário e modelos de relatório de utilização podem modificar o período de retenção do relatório (para sempre, 7 dias, 30 dias, 90 dias).
5. Na guia **EMAIL**, os e-mails podem ser adicionados ou removidos manualmente da lista *When report is finished* e/ou da lista *If an error occurs*.
6. Selecione **APPLY** e/ou **OK**.

Gerando relatórios de SMT

Um relatório SMT pode ser gerado após a última etapa do assistente Create Report ou selecionando um modelo de relatório listado na tabela de nomes Template e selecionando **Run Report**.

Sobre esta tarefa

Os agendamentos podem ser consolidados em vários sistemas Data Domain e PowerProtect da seguinte maneira:

- Se dois ou mais agendamentos tiverem o mesmo nome, tipo e agendamento (por exemplo, "todas as segundas-feiras, às 7h"), o DDMC exibirá um agendamento configurado em sistemas diferentes.
- Se dois agendamentos tiverem o mesmo nome, mas tipos e/ou horários agendados diferentes, o DDMC exibirá dois agendamentos.
- Se um agendamento estiver *Disabled* em um sistema, mas *Enabled* em outro, o DDMC exibirá um agendamento.

Etapas

1. Selecione **Reports** > **Management**.
2. Selecione um modelo de relatório na lista.
3. Selecione Run Report.

Resultados

Um relatório (denominado pela concatenação do registro de data para o título do modelo) é criado e aberto como um arquivo PDF no navegador, exceto para o relatório de utilização do tenant, que é gerado como um arquivo do Excel.

As informações de geração de relatório são listadas na tabela Report History, em que ele pode ser visualizado, renomeado ou excluído.

7

Fazendo configurações adicionais

Tópicos:

- Gerenciando configurações de rede
- Gerenciando o acesso ao DDMC
- Gerenciando definições de configuração geral
- Atualizando o software DDMC

Gerenciando configurações de rede

A página **Settings** apresenta informações sobre o status e a configuração de interfaces de rede, DNS, hosts, SNMP (Simple Network Management Protocol) e rotas. As configurações podem ser acessadas por meio do ícone de engrenagem no banner do DDMC, no canto superior direito. Use essa área para configurar o sistema de rede para o DDMC.

Definindo configurações de rede

Use o ícone de engrenagem no banner do DDMC para acessar **Settings**, que são exibidas em um menu suspenso para usuários admin e limited-admin. Selecione uma das opções em **Network**.

Conceitos relacionados

Configurando interfaces de rede na página 86
Configurando rotas na página 90

Exibindo as configurações de rede

Você pode visualizar as configurações de rede do DDMC, ao mesmo tempo que adiciona ou remove as configurações.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione uma das opções em Network.
2. Visualize as configurações de rede (descritas na tabela a seguir) e use o botão de adicionar, editar ou excluir para alterar a configuração.

Tabela 15. Configurações de rede

Item	Descrição
Interface	
Status	Habilitar ou desabilitar a interface
Configurações de IP	Defina o modo: DHCPv4, DHCPv6 ou manual
Velocidade/duplex	Defina o modo de negociação automática ou manual, velocidade, e duplex
MTU	Modo padrão ou manual
Hosts	
Mode	Especifique se deseja usar um endereço de gateway de DHCP ou um endereço IP configurado estaticamente
Nome de host	Nome de host do sistema DD selecionado

Tabela 15. Configurações de rede (continuação)

Item	Descrição
Domain name	Nome do domínio completo que está associado ao sistema DD selecionado
Mapeamento	Adicionar, editar ou excluir hosts que estão conectados ao DDMC
DNS	
Servidores DNS	Especifique se deseja usar o DHCP ou adicionar, editar ou excluir manualmente os endereços IP estáticos de servidores DNS
Domínio de pesquisa	Lista de domínios de pesquisa que são usados por um sistema. O sistema aplica o domínio de pesquisa como um sufixo ao nome de host.
Rotas	
Rotas estáticas	
Gateway IPv4	Especifique se deseja usar um endereço de gateway de DHCP ou um endereço IP configurado estaticamente
Gateway IPv6	Especifique se deseja usar um endereço de gateway de DHCP ou um endereço IP configurado estaticamente
Rotas estáticas	Adicione, edite ou exclua rotas estáticas, especificando a interface, o destino e o gateway
Rotas dinâmicas	
Rotas dinâmicas	Visualize uma lista de rotas dinâmicas atribuídas pelo sistema.
SNMP (Simple Network Management Protocol)	
Status	Habilitar ou desabilitar SNMP
Localização	Especifique o local do SNMP
Contact	Especifique o contato do SNMP
Configuração do V3	Adicione, edite ou exclua usuários e hosts de trap do SNMP V3
Configuração do V2C	Adicione, edite ou exclua as comunidades e hosts de trap do SNMP V2C

Conceitos relacionados

Gerenciando uma lista de pesquisa do domínio na página 90
Mapeando hosts na página 88
Definindo configurações do DNS na página 89

Tarefas relacionadas

Configurando hosts na página 87

Configurando interfaces de rede

Você pode modificar as conexões físicas de rede e as configurações existentes de interface do DDMC na página **Settings**.

Conceitos relacionados

Definindo configurações de rede na página 85
Configurando rotas na página 90

Visualizando informações da interface

A página Interfaces (**Settings** > **Network** > **guia Interface**) permite gerenciar e configurar a interface física (Ethernet), DHCP, DDNS e endereços IP e exibe informações e o status da rede.

Há duas partes nesta página: a área Interfaces e a área Details. Selecione uma interface e clique em **Edit** para modificar uma interface.

Tabela 16. Área de interfaces

Item	Descrição
Interface	Nome de cada interface Ethernet associada ao DDMC. Os nomes de interfaces físicas iniciam com `eth`.
Status	Permite que você visualize ou altere o status de interface.
DHCP	Indica se a interface está configurada com um endereço IP de um servidor DHCP (Dynamic Host Configuration Protocol).
Endereço IP	Endereço IP associado à interface, que é usado pela rede para identificar a interface. Se a interface estiver configurada com DHCP, um asterisco é mostrado depois desse valor.
Máscara de rede	Máscara de rede associada à interface. Usa o formato padrão para máscaras de rede IP. Se a interface estiver configurada com DHCP, um asterisco é mostrado depois desse valor.
Link	Indica se o link de Ethernet física está ativo.
Additional Info	Fornece configurações adicionais da interface, por exemplo, o modo de vinculação.

Para preencher a área Details, selecione uma interface.

Tabela 17. Área Details

Item	Descrição
Interface Name	Nome da interface selecionada.
Hardware Address	Endereço MAC de interface selecionada, por exemplo, `00:02:b3:b0:8a:d2`
Cabo	Indica se a interface é de cobre ou fibra óptica.
MTU	Valor da Unidade máxima de transmissão atribuído à interface.
Autonegotiate	Indica se a interface está habilitada para negociar automaticamente as configurações de velocidade e duplex. Se estiver desabilitada, os valores de velocidade e duplex são definidos manualmente.
Duplex	Protocolo usado com o valor de velocidade, que define o protocolo de transferência de dados. Os valores são Unknown, Full ou Half.
Velocidade	Protocolo usado com o valor Duplex, que define a taxa de transferência de dados. As opções são Unknown, 10 Mb/s, 100 Mb/s, 1000 Mb/s ou 10 Gb/s.
Supported Speeds	Lista todas as velocidades que a interface é capaz de usar.

Configurando hosts

O nome do host e o nome de domínio são usados por outros sistemas quando desejam acessar o DDMC. O nome do host pode ser definido manualmente ou automaticamente gerado com DHCP.

Sobre esta tarefa

Observe o seguinte antes de configurar um host ou nome de domínio:

- Não inclua underline no nome do host. Ele é incompatível com alguns navegadores.
- Alterar os nomes de um host ativo pode causar: (1) uma interrupção na conexão atual (se isso acontecer, faça log-in novamente e verifique as configurações salvas) e/ou (2) interrupção da comunicação com os sistemas gerenciados.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Network** > **Hosts**.
2. Selecione como deseja definir os nomes de host e de domínio:
   - **Obter configurações usando DHCP.**

- **Manualmente.**
  - Digite um nome do host.
  - Digite um nome do domínio, que é o nome do domínio associado ao DDMC. Geralmente, esse é o nome do domínio de sua empresa. Por exemplo, `yourcompany.com`

3. Clique em **Apply**.

Conceitos relacionados

Gerenciando uma lista de pesquisa do domínio na página 90
Mapeando hosts na página 88
Definindo configurações de DNS na página 89

Tarefas relacionadas

Exibindo as configurações de rede na página 85

Mapeando hosts

Use a área Hosts Mapping para adicionar um mapeamento que vincule um endereço IP a um nome de host.

O mapeamento de hosts é necessário quando o DNS não está configurado. O DNS mapeia o nome de um dispositivo com seu endereço IP. Se o DDMC não estiver configurado no DNS (e se os sistemas não estiverem configurados para usar o DNS), o mapeamento de hosts será necessário.

Conceitos relacionados

Gerenciando uma lista de pesquisa do domínio na página 90
Definindo configurações de DNS na página 89

Tarefas relacionadas

Exibindo as configurações de rede na página 85
Configurando hosts na página 87

Adicionando um mapeamento do nome do host

Você pode adicionar um mapeamento do nome do host, enquanto adiciona um nome do host, se necessário.

Etapas

1. Selecione **ADD** na área Mapeamento de hosts para criar um mapeamento de host.
2. Se nenhum host estiver listado na lista Host Name, selecione o botão adicionar (+).
3. Na caixa de diálogo **Add Host**, digite um endereço IP e um ou mais nomes de host que serão usados para o mapeamento.

   O novo nome do host é adicionado à lista de Host Names. Continue a adicionar nomes do host conforme necessário.

4. Selecione **ADD**.

   O mapeamento é criado e você retornará à página de hosts.

5. Para salvar o recém-criado mapeamento de host, clique em **APPLY**.

Tarefas relacionadas

Excluindo um mapeamento do nome do host na página 88

Excluindo um mapeamento do nome do host

Você pode excluir um mapeamento do nome de host na tabela de nomes de host.

Etapas

1. Na tabela **Mapping**, selecione as linhas que deseja excluir.
2. Clique no botão **Delete** acima da tabela Mapping.
3. Clique em **APPLY** para salvar as alterações.
4. Selecione **Close** quando for exibida a mensagem Complete.
   Você retornará à guia Settings.

Tarefas relacionadas

Adicionando um mapeamento do nome do host na página 88

Definindo configurações de DNS

As configurações de DNS podem ser configuradas na página **Settings**, que é acessada clicando no ícone de engrenagem, no canto superior direito.

Conceitos relacionados

Gerenciando uma lista de pesquisa do domínio na página 90
Mapeando hosts na página 88

Tarefas relacionadas

Exibindo as configurações de rede na página 85
Configurando hosts na página 87

Adicionando um endereço IP do DNS

Os servidores DNS são exibidos em uma tabela com opções de botão Add e Delete.

Etapas

1. Determine o método para obter o DNS. Escolha se deseja:
   - Obter configurações de DNS usando DHCP. (Pelo menos uma interface deve ser configurada com o uso do DHCP.)
   - Configurar o DNS manualmente:
   a. Selecione o botão do sinal de adição (**+**).
   b. Informe o endereço IP do DNS.
2. Selecione **APPLY** para salvar as alterações.

Tarefas relacionadas

Excluindo um endereço IP do DNS na página 89

Excluindo um endereço IP do DNS

Os servidores DNS são exibidos em uma tabela com opções de botão Add e Delete.

Etapas

1. Selecione uma ou mais linhas a partir da lista da tabela.
2. Clique no botão Delete (**X**), no endereço IP de DNS na tabela a ser excluída.
3. Selecione **Apply** para salvar as alterações.

Tarefas relacionadas

Adicionando um endereço IP do DNS na página 89

Gerenciando uma lista de pesquisa do domínio

Você pode adicionar ou remover um domínio de uma lista de pesquisa de domínio.

Conceitos relacionados

Mapeando hosts na página 88
Definindo configurações de DNS na página 89

Tarefas relacionadas

Exibindo as configurações de rede na página 85
Configurando hosts na página 87

Adicionando um domínio de pesquisa

Os domínios de pesquisa são exibidos como uma tabela Action, na página DNS.

Etapas

1. Clique no botão **Add** (+), ao lado de "Search domain names".
2. Digite um nome na caixa de texto "Search domain".
3. Selecione **Add**.

Resultados

Você deve retornar para a página DNS, com o Search Domain recém-adicionado à lista.

Tarefas relacionadas

Removendo um domínio de pesquisa na página 90

Removendo um domínio de pesquisa

Os domínios de pesquisa são exibidos como uma tabela Action, na página DNS.

Etapas

1. Selecione os domínios de pesquisa a serem excluídos da lista "Search domain names".
2. Clique no botão **Delete** (X), acima da tabela.
3. Selecione **Apply**.

Resultados

As alterações são aplicadas ao sistema.

Tarefas relacionadas

Adicionando um domínio de pesquisa na página 90

Configurando rotas

As rotas determinam o caminho usado para transferir dados para e do host local (DDMC) para outra rede ou host.

O DDMC não gera e nem responde a nenhum protocolo de gerenciamento de roteamento de rede (RIP, EGRP/EIGRP e BGP). O único roteamento implementado no DDMC é baseado na tabela de rotas internas, onde o administrador pode definir uma rede específica ou uma sub-rede utilizada por uma interface física (ou grupo de interfaces).

O DDMC utiliza *roteamento baseado na origem*, o que significa que pacotes de rede de saída correspondentes à sub-rede de várias interfaces serão roteados pela interface física da qual se originaram.

NOTA: O roteamento de conexões iniciadas no DDMC (como para replicação) depende do endereço de origem usado para interfaces que usam a mesma sub-rede. Para forçar o tráfego de uma interface específica para um destino específico (mesmo se a interface estiver na mesma sub-rede que as outras), você pode configurar uma entrada de roteamento estático entre os dois sistemas que vão sobrepor o roteamento de origem.

Conceitos relacionados

Configurando interfaces de rede na página 86
Definindo configurações de rede na página 85

Visualizando informações da rota

As páginas Rotas fornecem detalhes sobre todas as informações de roteamento para configuração de seu DDMC, inclusive os valores de gateway padrão e as rotas estáticas e dinâmicas.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Network** > **Routes**.
2. Na página Routes, visualize as rotas estáticas e dinâmicas configuradas (descritas na tabela a seguir) e crie ou modifique as informações de roteamento.

Tabela 18. Informações de rota

item	description
Default IPv4 Gateway	Endereço do gateway padrão IPv4.
Default IPv6 Gateway	Endereço do gateway padrão IPv6.
Rotas estáticas	Rotas estáticas que são baseadas no host ou na rede.
Especificação da rota	Especificação da rota que está sendo usada para configurar rotas.
Rotas dinâmicas	Rotas atribuídas dinamicamente que utilizam caminhos de rede ou host para transmissão de dados.
Destination	Rede/host de destino para onde o tráfego de rede (dados) é enviado.
Gateway do	O endereço do roteador na rede DDMC ou 0.0.0.0 se nenhum gateway for definido.
Máscara de rede	Máscara de rede para a rede de destino. Defina inicialmente 255.255.255.255 para um destino de host e 0.0.0.0 para a rota padrão.
Indicadores	Os valores possíveis são: U — a rota está ativa. H — o destino é um host. G — usar gateway. R — restabelecer rota para roteamento dinâmico. D — instalado dinamicamente por daemon ou redirecionar. M — modificado de roteamento de daemon ou redirecionar. A — instalado por addrconf. C — entrada de cache. ! — rejeitar rota.
Medição	Distância até o destino (geralmente contada em nós de rede). (Não é usado pelo DD OS, mas pode ser necessário pelo roteamento de daemons.)
MTU	Tamanho da unidade máxima de transmissão (MTU) para a interface (Ethernet) física.
Janela	Tamanho da janela padrão para conexões TCP nesse rota.
IRTT	RTT (Round Trip Time, ciclo de ida e volta) inicial. O kernel utiliza este para estimar os melhores parâmetros do protocolo TCP sem esperar por respostas (possivelmente lentas).
Interface	Nome da interface associado à interface de roteamento.

Tarefas relacionadas

Configurando o endereço do gateway padrão IPv4 ou IPv6 na página 92
Criando rotas estáticas na página 92
Excluindo rotas estáticas na página 92

Configurando o endereço do gateway padrão IPv4 ou IPv6

Você pode definir o endereço do gateway padrão IPv4 ou IPv6 usando o servidor DHCP ou configurando-o manualmente.

Etapas

1. O Gateway padrão IPv4 ou o Gateway padrão IPv6 pode ser definido usando o valor DHCP ou um gateway configurado manualmente.
   a. **Use DHCP value**: indica que você deseja usar o valor do servidor DHCP (Dynamic Host Configuration Protocol).
   b. **Manually Configure**: indica que você deseja configurar manualmente o endereço do gateway e habilita a caixa **Gateway**, na qual você deve especificar o endereço do gateway. A alteração do modo de DHCP para Manual disponibilizará uma caixa de texto para especificar o gateway padrão.
2. Clique em **Apply** para salvar as alterações.

Tarefas relacionadas

Visualizando informações da rota na página 91
Criando rotas estáticas na página 92
Excluindo rotas estáticas na página 92

Criando rotas estáticas

Para forçar o tráfego de uma interface específica para um destino específico (mesmo que essa interface esteja na mesma sub-rede que outras interfaces), você pode configurar uma entrada de roteamento estático entre os dois sistemas que sobrepõem o roteamento de origem.

Etapas

1. Selecione **ADD** na tabela de ação Static Routes para criar uma rota.
2. Na caixa de diálogo Add Static Routes, selecione uma interface.
3. Especifique o **destino** selecionando uma das seguintes opções:
   - **Network** — digite o endereço IP da rede e a máscara de rede.
     NOTA: Esse não é o endereço IP da interface.
   - **Host** — digite o nome do host ou o endereço IP do host de destino da rota.
4. Opcionalmente, digite um novo endereço de gateway na caixa **Gateway**.
5. Selecione **Add** para fechar a caixa de diálogo e salvar as alterações.

   A nova rota agora foi adicionada à tabela Static Routes, na página Routes.
6. Para salvar o Route Spec recém-criado, clique em **APPLY**.

Tarefas relacionadas

Visualizando informações da rota na página 91
Configurando o endereço do gateway padrão IPv4 ou IPv6 na página 92
Excluindo rotas estáticas na página 92

Excluindo rotas estáticas

Você pode excluir rotas estáticas quando não precisar mais delas.

Etapas

1. Na área **Route Spec**, selecione da rota a ser excluída.

2. Selecione **Delete**.

   A caixa de diálogo Delete Route é exibida.

3. Selecione **Delete** e **Close**.

   A especificação de rota é removida da lista Route Spec.

4. Clique em **Apply** para salvar as alterações na lista de rotas.

Tarefas relacionadas

Visualizando informações da rota na página 91
Configurando o endereço do gateway padrão IPv4 ou IPv6 na página 92
Criando rotas estáticas na página 92

Trabalhando com o SNMP

Para monitorar o DDMC usando o SNMP, será necessário instalar o DD MIB em seu sistema de Gerenciamento do SNMP. O DD MIB permitirá SNMP consultas sobre informações específicas do DD.

O DDMC também é compatível com o padrão MIB-II, de modo que também seja possível consultar estatísticas da MIB-II para dados gerais, tais como estatísticas de rede. Para a cobertura completa de dados disponíveis, você deve utilizar o Data Domain MIB e o padrão MIB-II MIB.

O DDMC é compatível com SNMP V2C e/ou SNMP V3. O SNMP V3 fornece um grau maior de segurança do que o V2C substituindo strings de comunidade de texto não criptografadas (como um meio de autenticação), sendo que a autenticação baseada no usuário utiliza MD5 ou SHA1. Também com o SNMP V3, pacotes de autenticação de usuário podem ser criptografados e sua integridade verificada com DES ou AES.

A porta padrão aberta quando o SNMP está ativado é a porta 161. As traps são enviadas pela porta 162.

Tarefas relacionadas

Definindo configurações do servidor de e-mail na página 119
Configurando definições de data e hora na página 118
Configurando propriedades do sistema na página 118

Verificando o status e a configuração do SNMP

A página SNMP mostra o status e as propriedades do SNMP, além da configuração do SNMP V3 e do SNMP V2C.

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Network** > **SNMP**.
2. Visualize as informações sobre o SNMP, conforme descrito nas tabelas a seguir.

Tabela 19. Status do SNMP

Item	Descrição
Status	Status operacional do agente do SNMP no DDMC Management Center: Enabled ou Disabled.

Tabela 20. Propriedades do SNMP

Item	Descrição
Local do sistema SNMP	Local do DDMC.
Contato do sistema SNMP	Administrador do DDMC.

Tabela 21. Configuração do SNMP V3

Item	Descrição
Usuários do SNMP	
Nome	Nome do usuário no Gerenciador do SNMP com acesso ao agente do DDMC.

Tabela 21. Configuração do SNMP V3 (continuação)

Item	Descrição
Acesso	Permissões de acesso para o usuário SNMP: • Somente leitura • Leitura/gravação
Protocolos de autenticação	Protocolo de autenticação para validar o usuário SNMP: • MD5 • SHA1 • Nenhuma
Privacy Protocol	Protocolo de criptografia para validar o usuário SNMP: • AES • DES • Nenhuma
Hosts de trap	
Host	Endereço IP ou nome de domínio do host de gerenciamento do SNMP.
Porta	Porta usada para a comunicação do trap SNMP com o host. O padrão é a Porta 162.
Usuário	Usuário no host de trap autenticado para acessar as informações de SNMP.

Tabela 22. Configuração do SNMP V2C

Item	Descrição
Comunidades	
Comunidade	Nome da comunidade, por exemplo, Comunidade pública, privada ou local.
Acesso	Permissão de acesso atribuída: • Somente leitura • Leitura/gravação
Hosts	Os hosts nesta comunidade.
Hosts de trap	
Host	Sistemas designados para receber traps SNMP gerados pelo DDMC. Se esse parâmetro for configurado, os sistemas recebem mensagens de alerta, mesmo que o agente do SNMP esteja desativado.
Porta	Porta usada para a comunicação do trap SNMP com o host. O padrão é a Porta 162.
Comunidade	Nome da comunidade, por exemplo, Comunidade pública, privada ou local.

Conceitos relacionados

Gerenciando usuários do SNMP V3 na página 96
Gerenciando hosts de trap SNMP V3 e V2C na página 97
Gerenciando comunidades do SNMP V2C na página 98

Tarefas relacionadas

Habilitando ou desabilitando o SNMP na página 94
Fazendo download do MIB do SNMP na página 95
Configurando propriedades SNMP na página 95

Habilitando ou desabilitando o SNMP

Você pode habilitar ou desabilitar o SNMP por meio do DDMC.

Etapas

1. Na área Status, selecione **Enable** para usar o SNMP.
2. Na área Status, selecione **Disable** para interromper o uso do SNMP.
3. Clique em **Apply** para salvar as alterações.

Conceitos relacionados

Verificando o status e a configuração do SNMP na página 93
Gerenciando usuários do SNMP V3 na página 96
Gerenciando hosts de trap SNMP V3 e V2C na página 97
Gerenciando comunidades do SNMP V2C na página 98

Tarefas relacionadas

Fazendo download do MIB do SNMP na página 95
Configurando propriedades SNMP na página 95

Fazendo download do MiB do SNMP

Você pode baixar o MIB do SNMP pelo DDMC.

Sobre esta tarefa

Na área Status, clique em **Download MiB file**.

Conceitos relacionados

Verificando o status e a configuração do SNMP na página 93
Gerenciando usuários do SNMP V3 na página 96
Gerenciando hosts de trap SNMP V3 e V2C na página 97
Gerenciando comunidades do SNMP V2C na página 98

Tarefas relacionadas

Habilitando ou desabilitando o SNMP na página 94
Configurando propriedades SNMP na página 95

Configurando propriedades SNMP

Você pode configurar o local do sistema SNMP e os contatos do sistema.

Etapas

1. Nos campos de texto SNMP, adicione um local do sistema SNMP (uma descrição de onde se encontra o DDMC) e/ou um contato do sistema SNMP (por exemplo, o endereço de e-mail do administrador do sistema para o DDMC).
2. Clique em **Apply** para salvar as alterações.

Conceitos relacionados

Verificando o status e a configuração do SNMP na página 93
Gerenciando usuários do SNMP V3 na página 96
Gerenciando hosts de trap SNMP V3 e V2C na página 97
Gerenciando comunidades do SNMP V2C na página 98

Tarefas relacionadas

Habilitando ou desabilitando o SNMP na página 94
Fazendo download do MiB do SNMP na página 95

Gerenciando usuários do SNMP V3

Procedimentos de gerenciamento de usuários do V3, inclusive criação, modificação e remoção de contas de usuário. Os usuários no gerenciador do SNMP têm acesso ao agente do DDMC.

Conceitos relacionados

Verificando o status e a configuração do SNMP na página 93
Gerenciando hosts de trap SNMP V3 e V2C na página 97
Gerenciando comunidades do SNMP V2C na página 98

Tarefas relacionadas

Habilitando ou desabilitando o SNMP na página 94
Fazendo download do MIB do SNMP na página 95
Configurando propriedades SNMP na página 95

Criando usuários do SNMP V3

Você pode configurar usuários SNMP (Simple Network Management Protocol) V3 usando a tabela Action, na página SNMP Settings.

Etapas

1. Na área V3 Configuration Users, selecione **ADD**.
2. No campo Name, digite o nome do usuário ou o gerenciador do SNMP que terá acesso ao agente do DDMC. O nome deve ter no mínimo 8 caracteres.
3. Selecione o acesso somente leitura ou leitura-gravação para esse usuário.
4. Para autenticar o usuário, marque a caixa de seleção **Authentication**.
   a. Selecione o protocolo MD5 ou o SHA1.
   b. Digite a chave de autenticação no campo de texto Key.
   c. Para fornecer criptografia para a sessão de autenticação, selecione a caixa de seleção ao lado de **Privacy**.
   d. Selecione o protocolo AES ou DES.
   e. Digite a chave de criptografia no campo de texto Key.
5. Selecione **APPLY**.

   A conta de usuário recém-adicionada aparece na tabela SNMP V3 Users.

Tarefas relacionadas

Modificando usuários do SNMP V3 na página 96
Removendo usuários do SNMP V3 na página 97

Modificando usuários do SNMP V3

Você pode modificar uma variedade de informações sobre os usuários do SNMP V3.

Etapas

1. Na tabela Action, na seção V3 Configuration, na página SNMP Configuration, selecione **EDIT**.
2. Selecione o acesso somente leitura ou leitura-gravação para esse usuário.
3. Para autenticar o usuário, marque a caixa de seleção **Authentication**.
   a. Selecione o protocolo MD5 ou o SHA1.
   b. Digite a chave de autenticação no campo de texto Key.
   c. Para fornecer criptografia para a sessão de autenticação, selecione a caixa de seleção ao lado de **Privacy**.
   d. Selecione o protocolo AES ou DES.
   e. Digite a chave de criptografia no campo de texto Key.
4. Selecione **APPLY**.

As novas configurações para essa conta de usuário são exibidas na tabela Usuários do SNMP.

Tarefas relacionadas

Criando usuários do SNMP V3 na página 96
Removendo usuários do SNMP V3 na página 97

Removendo usuários do SNMP V3

Se um usuário do SNMP V3 estiver sendo usado por um ou mais hosts de trap, você deve primeiro excluir os hosts de trap antes de excluir o usuário.

Etapas

1. Na tabela Action, na seção V3 Configuration, na página SNMP Configuration, selecione **DELETE**.
2. Verifique o nome do usuário que será excluído e selecione **APPLY**.

   NOTA: Se o botão **DELETE** estiver desabilitado, o usuário selecionado está sendo usado por um ou mais hosts de trap. Exclua os hosts de trap e, em seguida, exclua o usuário.

A conta de usuário é removida da tabela de SNMP Users.

Tarefas relacionadas

Criando usuários do SNMP V3 na página 95
Modificando usuários do SNMP V3 na página 96

Gerenciando hosts de trap SNMP V3 e V2C

O gerenciamento de hosts de trap SNMP V3 e V2C inclui criar, modificar e remover hosts que receberam traps SNMP.

Conceitos relacionados

Verificando o status e a configuração do SNMP na página 93
Gerenciando usuários do SNMP V3 na página 95
Gerenciando comunidades do SNMP V2C na página 98

Tarefas relacionadas

Habilitando ou desabilitando o SNMP na página 94
Fazendo download do MIB do SNMP na página 95
Configurando propriedades SNMP na página 95

Criando hosts de trap SNMP V3 e V2C

Você pode criar hosts SNMP (Simple Network Management Protocol) V3 e V2C trap usando a tabela de ação na página SNMP Settings.

Etapas

1. Na área de SNMP V3 Trap Hosts ou SNMP V2C Trap Hosts, clique em **ADD**.
2. No campo de texto Host, informe o endereço IP ou nome do domínio do host SNMP para onde os traps serão enviados.
3. No campo de texto Port, digite o número da porta para o envio de traps (162 é uma porta usada com frequência).
4. Selecione o usuário (SNMP V3) ou a comunidade (SNMP V2C) no menu drop-down.

   Como alternativa, no menu drop-down, selecione Create New User (SNMP V3) para adicionar um usuário SNMP ou Create New Community (SNMP V2C) para adicionar uma comunidade SNMP.
5. Selecione **APPLY**.

Tarefas relacionadas

Modificando hosts de trap SNMP V3 e V2C na página 98
Removendo hosts de trap SNMP V3 e V2C na página 98

Modificando hosts de trap SNMP V3 e V2C

Você pode modificar a porta, usuário e/ou comunidade de um host de trap SNMP V3 ou V2C usando a tabela Action, na página SNMP Settings.

Etapas

1. Na área Trap Hosts (para V3 ou V2C), selecione uma entrada do Trap Host e selecione **Edit**.

   A caixa de diálogo **Edit SNMP [V3 or V2C] Trap Hosts** é exibida. Modifique qualquer um dos itens a seguir.

2. No campo de texto Port, digite o número de porta para o envio de traps (162 é uma porta usada com frequência).
3. Selecione o usuário (SNMP V3) ou a comunidade (SNMP V2C) no menu drop-down.
4. Selecione **Apply**.

Tarefas relacionadas

Criando hosts de trap SNMP V3 e V2C na página 97
Removendo hosts de trap SNMP V3 e V2C na página 98

Removendo hosts de trap SNMP V3 e V2C

Você pode remover hosts de trap SNMP V3 e V2C usando a tabela Action, na página SNMP Settings.

Etapas

1. Na área Trap Hosts (para V3 ou V2C), selecione uma entrada para o host de trap e selecione **Delete**.
2. Verifique o nome do host que será excluído e clique em **Apply**.

   A entrada do host de trap é removida da tabela Trap Hosts.

Tarefas relacionadas

Criando hosts de trap SNMP V3 e V2C na página 97
Modificando hosts de trap SNMP V3 e V2C na página 98

Gerenciando comunidades do SNMP V2C

A string de comunidade é enviada em um texto não criptografado e é muito fácil de interceptar. Se isso ocorrer, o interceptor pode recuperar informações dos dispositivos na rede, modificar sua configuração e, possivelmente, encerrá-las. Em vez disso, o uso da configuração de usuários do SNMP V3 fornece autenticação e criptografia para evitar que isso aconteça.

Conceitos relacionados

Verificando o status e a configuração do SNMP na página 93
Gerenciando usuários do SNMP V3 na página 96
Gerenciando hosts de trap SNMP V3 e V2C na página 97

Tarefas relacionadas

Habilitando ou desabilitando o SNMP na página 94
Fazendo download do MIB do SNMP na página 95
Configurando propriedades SNMP na página 95

Criando comunidades do SNMP V2C

Você pode criar comunidades SNMP V2C usando a tabela Action, na página SNMP Settings.

Etapas

1. Na área Communities, clique em **ADD**.

   Será exibida a caixa de diálogo **Add V2C Community**.

2. No campo Community, digite o nome da comunidade do gerenciador do SNMP que terá acesso ao agente do DDMC. O nome da comunidade deve ter no mínimo 8 caracteres.
3. Selecione acesso somente leitura ou leitura e gravação para essa comunidade.
4. Na área Hosts, selecione a caixa de seleção de um host na lista ou:
   a. Selecione **+** para adicionar um host.
   b. Digite o endereço IP ou nome de domínio do host no campo de teste Hosts.

   O host é adicionado à lista de hosts.
5. Selecione **ADD**.

   A entrada da nova comunidade é exibida na tabela Comunidades.

Tarefas relacionadas

Modificando comunidades do SNMP V2C na página 99
Excluindo comunidades do SNMP V2C na página 99

Modificando comunidades do SNMP V2C

Você pode modificar comunidades SNMP V2C usando a tabela Action, na página SNMP Settings.

Etapas

1. Na área Communities, marque uma caixa de seleção da comunidade e clique em **EDIT**.

   Será exibida a caixa de diálogo **Edit V2C Community**. Adicione ou altere qualquer uma das configurações a seguir.

2. Selecione acesso somente leitura ou leitura e gravação para essa comunidade.
3. Na área Hosts, selecione a caixa de seleção de um novo host na lista ou:
   a. Selecione **+** para adicionar um host.

      A caixa de diálogo Host é exibida.
   b. No campo de texto Host, informe o endereço IP ou nome de domínio do host.
   c. Selecione **OK**.

   O host é adicionado à lista de hosts.
4. Selecione **Apply**.

   A entrada da comunidade modificada é exibida na tabela Communities.

Tarefas relacionadas

Criando comunidades do SNMP V2C na página 99
Excluindo comunidades do SNMP V2C na página 99

Excluindo comunidades do SNMP V2C

Se uma comunidade do SNMP V2C estiver sendo usada por um host de trap, você deve excluir o host de trap antes de poder excluir a comunidade.

Etapas

1. Na área Communities, marque uma caixa de seleção da comunidade e clique em **DELETE**.

NOTA: Se o botão **Delete** estiver desabilitado, a comunidade selecionada está sendo usada por um ou mais hosts de trap. Exclua os hosts de trap e depois exclua a comunidade.

2. Verifique o nome da comunidade que será excluída e selecione **APPLY**.
   A entrada da comunidade é removida da tabela Communities.

Tarefas relacionadas

Criando comunidades do SNMP V2C na página 99
Modificando comunidades do SNMP V2C na página 99

Gerenciando o acesso ao DDMC

O gerenciamento de acesso inclui a exibição e configuração dos serviços que fornecem acesso de administrador e usuário ao DDMC.

Funções necessárias para tarefas do DDMC

Quando a confiança mútua estiver estabelecida entre o DDMC e seus sistemas gerenciados, se um usuário for adicionado ao DDMC com acesso de nível *admin* ou *limited-admin*, este usuário também poderá acessar os sistemas gerenciados (por meio de ssh ou iniciando o DD System Manager para realizar operações de nível de administrador. Além disso, um usuário de nível de admin ou de limited-admin pode atualizar um sistema gerenciado. Portanto, cada novo usuário do DDMC deve receber a mesma consideração que receberia um novo usuário do DD System Manager.

As funções disponíveis no DDMC são as mesmas que as do DD System Manager:

- *admin*, o *administrador do DDMC*. Um administrador pode acessar todas as funções em uma página do DDMC.
- *limited-admin*, um *Administrador limitado do DDMC*. A função limited-admin pode configurar e monitorar o sistema DD com algumas limitações. Usuários com a função de limited-admin não podem:
  - realizar operações de exclusão de dados
  - editar o registro
  - excluir pacotes .rpm carregados por upload
  - excluir agendamentos de atualização
  - entrar no modo bash ou SE
- *usuário*, um *usuário do DDMC*. Um usuário, que pode ser um usuário independente ou parte de um grupo, tem acesso apenas a determinadas funções em uma página do DDMC, com base na função atribuída a esse usuário ou grupo.

A tabela a seguir mostra as ações disponíveis para cada recurso do DDMC. [Essa tabela é fornecida para mostrar quando somente a função de *usuário* é necessária. A função de *admin* pode executar todas as tarefas, conforme mencionadas anteriormente.]

Tabela 23. Funções do DDMC necessárias para tarefas do DDMC

Ação	Permissão mínima	Descrição de ações
Gerenciar permissões	• Administrador • Administrador limitado	Atribuir, editar, remover permissões para usuários. Observe que a função de administrador do DDMC ou o sistema associado não pode ser excluída na página de permissões.
Gerenciar sistemas DD	• Administrador • Administrador limitado	Adicionar, editar e excluir sistemas do inventário
Gerenciar usuários/grupos de usuários	• Administrador • Administrador limitado	Adicionar, editar e excluir usuários locais; o administrador também pode adicionar, editar e excluir grupos de usuários do AD/NIS e LDAP. Somente o usuário administrador pode adicionar, editar e excluir outro usuário com a mesma função.
Configurar o DDMC	• Administrador • Administrador limitado	Trabalhar com páginas de configurações do DDMC
Atualizar sistemas	No sistema que será atualizado: • Administrador	Executar a função de atualização do sistema

Tabela 23. Funções do DDMC necessárias para tarefas do DDMC (continuação)

Ação	Permissão mínima	Descrição de ações
	• Administrador limitado	
Atualizar DDMC	• Administrador • Administrador limitado	Executar a função de atualização do DDMC
Gerenciar grupos	• Administrador • Administrador limitado	Criar, editar, excluir grupos
Gerenciar propriedades	• Administrador • Administrador limitado	Criar, editar, excluir propriedades
Atribuir propriedades	• Administrador • Administrador limitado	Atribuir propriedades a sistemas
Atribuir a grupos	• Administrador	Atribuir sistemas a grupos
Gerenciar relatórios	• Administrador • Administrador limitado	Criar modelos de relatório e agendar a criação de relatório
Gerenciar recursos do painel de controle	• Administrador • Administrador limitado	Criar recursos do painel de controle
Configurar painel de controle	• Administrador • Administrador limitado	Configurar recursos e layouts do painel de controle
Gerenciar regras globais de filtro	• Usuário	Adicionar, editar e excluir regras de filtro
Visualizar o DD System Manager	• Usuário	Iniciar o DD System Manager virtual **NOTA:** É necessário privilégio de administrador no sistema gerenciado para alterar algo.
Gerenciar trabalhos do usuário	• Usuário	Suspender, retomar, cancelar trabalhos pertencentes ao usuário
Gerenciar todos os trabalhos	• Administrador	Suspender, retomar, cancelar qualquer trabalho
Gerenciar replicação avançada	• Administrador • Administrador limitado	Visualizar o status da replicação, exportar para arquivo CVS, atribuir propriedades
Gerenciar replicação básica	• Usuário	Visualizar o status da replicação, exportar para arquivo CVS

Conceitos relacionados

Gerenciar o acesso do usuário local ao DDMC na página 106

Gerenciando o acesso de administrador

O Administrator Access fornece configurações para definir como os usuários podem se conectar ao DDMC. Cada protocolo é configurado separadamente com o uso dos procedimentos desta seção.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Administrator Access**.
2. Visualize a **Passphrase** se ela estiver definida; se não estiver, defina-a. A Passphrase é uma chave de leitura humana (compreensível), como um smart card, que é usada para gerar uma chave de criptografia AES 256 utilizável pela máquina. (Para obter mais informações, consulte o *DD OS Administration Guide*). Você também pode ver os serviços disponíveis e, para um serviço selecionado, as opções de serviços configuradas para isso.

Tabela 24. Detalhes

Item	Descrição
Nome	Nome de um serviço/protocolo que pode acessar o sistema. Um dos seguintes protocolos pode ser selecionado (para visualização ou configuração): FTP, FTPS, HTTP/HTTPS, SCP/SSH ou Telnet.
Habilitado	Status do serviço: ativado ou desativado.
Allowed Hosts	Permissões de acesso definidas para o host designado.

Tabela 25. Opções de protocolo

Nome do protocolo	Nome da opção	Descrição
FTP	Timeout de sessão	Número configurado de segundos decorridos antes que o serviço encerre a sessão ou Infinite.
FTPS	Timeout de sessão	Número configurado de segundos decorridos antes que o serviço encerre a sessão ou Infinite.
HTTP/HTTPS	Porta HTTP/HTTPS	Se aplicável, número da porta aberta para o protocolo HTTP/HTTPS (HTTP — porta 80, por padrão; HTTPS — porta 443, por padrão).
	Timeout de sessão	Número configurado de segundos decorridos antes que o serviço encerre a sessão ou Infinite.
SCP/SSH	Porta SCP/SSH	Se aplicável, número da porta aberta para o protocolo SCP/SSH (porta 22, por padrão).
	Timeout de sessão	Número configurado de segundos decorridos antes que o serviço encerre a sessão ou Infinite.
Telnet	Timeout de sessão	Número configurado de segundos decorridos antes que o serviço encerre a sessão ou Infinite.

Gerenciando o acesso ao FTP

Você pode fornecer acesso ao DDMC por meio de uma conexão FTP.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Administrator Access**.
2. Na área **Services**, selecione FTP e clique em **Edit**.
3. Na caixa de diálogo Access, selecione **Enabled** ou **Disabled**. Se o FTPS estiver habilitado, ele será desabilitado antes de habilitar o FTP.
4. Em **Session Timeout**, digite, em segundos, o intervalo que deve transcorrer antes do encerramento da conexão ou escolha o padrão **Infinite**.
5. Determine como os hosts devem se conectar:
   - **Todos os hosts**
   - **Specified hosts** — nomes do host podem ser um nome do host totalmente qualificado ou um endereço IP.
     - Para adicionar um host, selecione Add (sinal de mais verde). Digite o nome do host e clique em **Save**.
     - Para modificar um nome de host, selecione o nome do host na lista **Hosts**, clique em Edit (lápis), altere-o e clique em **Save**.
     - Para remover um nome do host, selecione o nome do host na lista **Hosts**, clique em Delete (X) e em **Save**.
6. Clique em **Apply** para salvar as alterações.

Gerenciando o acesso ao FTPS

Você pode fornecer acesso ao DDMC por meio de uma conexão FTPS.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Administrator Access**.
2. Na área **Services**, selecione FTPS e clique em **Edit**.
3. Na caixa de diálogo Access, selecione **Enabled** ou **Disabled**. Se o FTP estiver habilitado, ele será desabilitado antes de habilitar o FTPS.
4. Em **Session Timeout**, digite, em segundos, o intervalo que deve transcorrer antes do encerramento da conexão ou escolha o padrão de **Infinite**. Para retornar aos valores padrão, selecione o botão **Default**.
5. Determine como os hosts devem se conectar:
   - **Todos os hosts**
   - **Specified hosts** — nomes do host podem ser um nome completo do host ou um endereço IP.
     - Para adicionar um host, selecione Add (sinal de mais verde). Digite o nome do host e clique em **Save**.
     - Para modificar um nome de host, selecione o nome do host na lista **Hosts**, clique em Edit (lápis), altere-o e clique em **Save**.
     - Para remover um nome de host, selecione o nome do host na lista **Hosts** e clique em Delete (X).
6. Clique em **Apply** para salvar as alterações.

Gerenciando acesso a HTTP/HTTPS

Você pode oferecer acesso ao DDMC por meio de uma conexão HTTP e/ou HTTPS.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Administrator Access**.
2. Na área **Services**, selecione **HTTP/HTTPS** e clique em **Edit**.
3. Na caixa de diálogo Edit HTTP/HTTPS Access, selecione **Enabled** ou **Disabled** e uma porta para HTTP e HTTPS.
4. Em **Session Timeout**, digite, em segundos, o intervalo que deve transcorrer antes do encerramento da conexão ou escolha **Infinite**. O valor padrão é 10.800 segundos (3 horas).
5. Determine como os hosts devem se conectar:
   - **Todos os hosts**
   - **Specified hosts** — nomes do host podem ser um nome completo do host ou um endereço IP.
     - Para adicionar um host, selecione Add (sinal de mais verde). Digite o nome do host e clique em **Save**.
     - Para modificar um nome de host, selecione o nome do host na lista **Hosts**, clique em Edit (lápis), altere-o e clique em **Save**.
     - Para remover um nome de host, selecione o nome do host na lista **Hosts**, clique em Delete (X) e em **Save**.
6. Clique em **Apply** para salvar as alterações.

Resultados

Tabela 26. HTTP/HTTPS ativado ou desativado

HTTP ativado	HTTPS ativado	Acesso ao DDMC por HTTP
X		Usa HTTP
	X	Mostra a página do servidor inativo
		Mostra a página do servidor inativo
X	X	Redireciona para o HTTPS

Gerenciando acesso SCP e SSH

Você pode oferecer acesso ao DDMC por meio de uma conexão SCP ou SSH.

Etapas

1. **NOTA:** A versão mínima suportada da OpenSSH do client SSH é OpenSSH v4.7p1.

   Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Administrator Access**.
2. Na área **Services**, selecione **SSH/SCP** e clique em **Edit**.
3. Na caixa de diálogo **Edit HTTP/HTTPS Access**, selecione **Enabled** ou **Disabled** e uma porta para SSH e SCP.
4. Em **Session Timeout**, digite, em segundos, o intervalo que deve transcorrer antes do encerramento de conexão ou escolha o valor padrão de **Infinite**.
5. Determine como os hosts devem se conectar:
   - **Todos os hosts**
   - **Specified hosts** — nomes do host podem ser um nome completo do host ou um endereço IP.
     - Para adicionar um host, selecione Add (sinal de mais verde). Digite o nome do host e clique em **Save**.
     - Para modificar um nome de host, selecione o nome do host na lista **Hosts**, clique em Edit (lápis), altere-o e clique em **Save**.
     - Para remover um nome de host, selecione o nome do host na lista **Hosts**, clique em Delete (X) e em **Save**.
6. Clique em **APPLY** para salvar as alterações.

Gerenciando o acesso ao telnet

Você pode fornecer acesso ao DDMC por meio de uma conexão Telnet.

Sobre esta tarefa

NOTA: Devido à conformidade FIPS, o Telnet pode ser desinstalado no DDMC por meio da CLI. Se for desinstalado, o Telnet não será parte da lista de protocolos no DDMC.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Administrator Access**.
2. Na área **Services**, selecione Telnet e clique em **Edit**.
3. Na caixa de diálogo Access, selecione **Enabled** ou **Disabled**.
4. Em **Session Timeout**, digite, em segundos, o intervalo que deve transcorrer antes do encerramento da conexão ou escolha o padrão de **Infinite**. Para retornar aos valores padrão, selecione o botão **Default**.
5. Determine como os hosts devem se conectar:
   - **Todos os hosts**
   - **Specified hosts** — nomes do host podem ser um nome completo do host ou um endereço IP.
     - Para adicionar um host, selecione Add (sinal de mais verde). Digite o nome do host e clique em **Save**.
     - Para modificar um nome de host, selecione o nome do host na lista **Hosts**, clique em Edit (lápis), altere-o e clique em **Save**.
     - Para remover um nome de host, selecione o nome do host na lista **Hosts**, clique em Delete (X) e em **Save**.
6. Clique em **Apply** para salvar as alterações.

Gerenciando certificados

Sobre esta tarefa

Certificados são gerenciados pela importação de arquivos raiz e intermediários de CA na GUI.

Arquivos de CA fornecem o seguinte:

- Permite somente aplicativos https para o tipo de host importado.
- O tipo de host importado permite que o tipo de arquivo importe um arquivo PKCS 12 (.p12), um arquivo público assinado (.pem) ou use texto de certificado.
- Pode fazer upload de um arquivo PKCS 12 (.p12) ou um arquivo público assinado (.pem) para o tipo de host importado.
- O arquivo p12 importado exige uma senha.
- O usuário tem a opção de gerar uma solicitação de assinatura de certificado ao selecionar a opção de tipo de arquivo .pem para o tipo de host importado.
- O usuário pode colar conteúdo de certificado na área de texto de certificado como certificado importado.

Arquivos intermediários de CA fornecem o seguinte:

- Permite somente aplicativos CA confiáveis para o tipo de CA importado.
- O tipo de CA importado permite que o tipo de arquivo importe um arquivo público assinado (.pem) ou use texto de certificado.

Etapas

1. Para importar a raiz de CA, digite o seguinte comando na CLI do Windows ou Linux:

```
ssh sysadmin@DDMC adminaccess certificate import ca application
login-auth < rootCA.crt
```

2. Para importar os arquivos intermediários da Autoridade de Certificação, digite o seguinte comando na CLI:

```
ssh sysadmin@DDMC adminaccess certificate import ca application
login-auth < intermediateCA.crt
```

Gerenciar o acesso do usuário local ao DDMC

A extensão na qual você pode gerenciar o acesso de usuário local ao DDMC depende de sua função.

Se você for um *administrador* no DDMC, será um *administrador global* e poderá configurar e monitorar todos os sistemas Data Domain e PowerProtect gerenciados.

Se você for um usuário no DDMC Management Center, poderá visualizar apenas os sistemas Data Domain gerenciados para os quais recebeu a função de user, *admin* ou *limited-admin* de um administrador do DDMC.

Conceitos relacionados

Funções necessárias para tarefas do DDMC na página 100

Tarefas relacionadas

Fazer log-in no DDMC na página 23

Visualizando informações do usuário local

Os registros de data no módulo de autenticação de usuário utilizam o horário de Greenwich (GMT). Portanto, ao configurar datas de expiração para desabilitar a conta e senha de um usuário, a data de expiração deve refletir o GMT em vez da hora local.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Local Users**.
2. Na página Local Users, visualize as informações dos usuários configurados.

Tabela 27. Informações para usuários configurados

Item	Descrição
Nome	ID do usuário, conforme adicionado ao sistema.
Função	Possíveis funções de usuários com base em um conjunto de privilégios: • *função admin*: pode configurar e monitorar todo o sistema. • *função limited-admin*: pode configurar e monitorar todo o sistema, mas não pode excluir/destruir dados do Mtree. • *função user*: pode monitorar sistemas e executar a operação de FastCopy. Os usuários com funções admin podem visualizar todos os usuários. Os usuários com funções user podem visualizar somente suas próprias contas de usuário.
Status	• enabled — o acesso do usuário à conta é permitido. • disabled — o acesso do usuário à conta é negado porque a data de expiração da conta foi atingida ou a senha de uma conta bloqueada não foi renovada. Usuários admin podem ativar ou desativar usuários com funções admin, limited-admin, ou user, exceto os usuários

Tabela 27. Informações para usuários configurados (continuação)

Item	Descrição
	SysAdmin. Nenhum usuário pode desabilitar o SysAdmin. Agentes de segurança podem habilitar/desabilitar somente outros agentes de segurança. • locked — o acesso do usuário à conta foi negado porque a senha expirou.
Disable Date	Data em que a conta está programada para ser desativada.
Last Login From	Localização do último log-in do usuário.
Last Login Time	Hora do último log-in do usuário.

3. Selecione um usuário específico para consultar informações detalhadas.

Tabela 28. Informações detalhadas de usuário específico

Item	Descrição
Password Last Changed	Data da última alteração da senha.
Minimum Days Between Change	Número mínimo de dias permitido ao usuário entre alterações de senha. O padrão é 0.
Maximum Days Between Change	Número máximo de dias permitido ao usuário entre alterações de senha. O padrão é 90.
Warn Days Before Expire	Número de dias de aviso aos usuários antes que a senha expire. O padrão é 7.
Disable Days After Expire	Número de dias após a expiração de uma senha para desabilitar a conta do usuário. O padrão é Never.

NOTA: A política de senha padrão pode ser alterada por um admin ou limited-admin selecionando **Manage Password Policies**. Os valores padrão são os valores iniciais padrão da política de senhas.

Conceitos relacionados

Funções de usuário na página 106

Tarefas relacionadas

Criando usuários locais na página 107
Modificando um perfil de usuário local na página 108
Excluindo um usuário local na página 108
Ativando ou desativando usuários locais na página 109
Alterando as senhas do usuário na página 109
Alterando opções de log-in na página 110

Funções de usuário

As funções oferecem um modo de restringir o acesso do usuário às funções do sistema usando um conjunto de privilégios. As permissões permitem que um admin ou um limited-admin tenha acesso a grupos e sistemas específicos, reduzindo a necessidade de configurar todos os usuários como um administrador global.

O DDMC é compatível com as seguintes funções:

- *função admin*: esta função pode configurar e monitorar todo o sistema.
  NOTA: É recomendável que a função de administrador seja usada criteriosamente e concedida a muito poucos usuários, pois esses usuários poderão configurar o DDMC, bem como ter acesso a todos os sistemas registrados.
- *função limited-admin*: essa função pode configurar e monitorar todo o sistema DDMC, mas não pode excluir ou destruir MTrees.
- *função user*: esta função pode monitorar o DDMC e sistemas para os quais o usuário tem permissão.

Tarefas relacionadas

Visualizando informações do usuário local na página 105
Criando usuários locais na página 107

Modificando um perfil de usuário local na página 108
Excluindo um usuário local na página 108
Ativando ou desativando usuários locais na página 109
Alterando as senhas do usuário na página 109
Alterando opções de log-in na página 110

Criando usuários locais

Você pode criar usuários com a função *admin*, *limited-admin* ou *user*.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Local Users**.
2. Clique em **Add**.
3. Na caixa de diálogo Add local User, digite o seguinte na guia General:

Tabela 29. Guia Geral

Item	Descrição
Nome	ID ou nome do usuário.
Função	Função de gerenciamento que é atribuída ao usuário: • *Administrator* e *limited-admin*: pode configurar e monitorar todo o DDMC e todos os sistemas Data Domain. • *User*: pode monitorar o DDMC e os sistemas para os quais eles têm permissão.

Password	Senha do usuário. Defina uma senha padrão e o usuário poderá alterá-la depois. O valor padrão para o comprimento mínimo de uma senha ou o número mínimo de classes de caracteres que são exigidos para a senha de um usuário é 9. Configuração de política de senha:
	• min-char-classes é 4, e não pode ser configurado
	• a senha deve ter pelo menos um:
	  ○ Caractere minúsculo (a-z)
	  ○ Caractere maiúsculo (A-Z)
	  ○ Caractere numérico (0-9)
	  ○ Caractere especial ($,%, #, + e assim por diante)
	• Por padrão, a senha não pode ter mais de três caracteres repetidos consecutivamente.

Verify Password	Senha do usuário novamente.
Disable account on the following date	Selecione **Manual** e digite uma data (mm/dd/aaaa) quando quiser desativar essa conta, ou use o valor padrão de never. Essa data utiliza GMT.
Minimum Days Between Change	Número mínimo de dias permitido ao usuário entre alterações de senha. O padrão é 0.
Maximum Days Between Change	Número máximo de dias permitido ao usuário entre alterações de senha. O padrão é 99,999.
Warn Days Before Expire	Número de dias de aviso aos usuários antes que a senha expire. O padrão é 7.
Disable Days After Expire	Número de dias após a expiração de uma senha para desabilitar a conta do usuário. O padrão é Never.

4. Selecione **Adicionar**.

   NOTA: A política de senha padrão pode ser alterada pelo admin ou pelo limited-admin usando **Manage Password Policies**. Os valores padrão são os valores iniciais padrão da política de senhas.

5. Clique em **Apply** para salvar as alterações.

Conceitos relacionados

Funções de usuário na página 106

Tarefas relacionadas

Visualizando informações do usuário local na página 105
Modificando um perfil de usuário local na página 108
Excluindo um usuário local na página 108
Ativando ou desativando usuários locais na página 109
Alterando as senhas do usuário na página 109
Alterando opções de log-in na página 110

Modificando um perfil de usuário local

Você pode modificar vários aspectos de um perfil de usuário local.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Local Users**.
2. Selecione um nome de usuário e clique em **Edit**.
3. Na caixa de diálogo Edit Local User: altere a função atribuída.
   a. Habilite ou desabilite o usuário.
   b. Altere a função do usuário.
   c. Altere a senha do usuário.
   d. Defina uma data para desabilitar o nome de usuário.
4. Opcionalmente, altere a política de expiração de senha para o usuário

Tabela 30. Política de expiração da senha

item	descrição
Minimum Days Between Change	Número mínimo de dias permitido ao usuário entre alterações de senha. O padrão é 0.
Maximum Days Between Change	Número máximo de dias permitido ao usuário entre alterações de senha. O padrão é 99999.
Warn Days Before Expire	Número de dias de aviso aos usuários antes que a senha expire. O padrão é 7.
Disable Days After Expire	Número de dias após a expiração de uma senha para desabilitar a conta do usuário. O padrão é Never.

5. Clique em **Save**.

Conceitos relacionados

Funções de usuário na página 106

Tarefas relacionadas

Visualizando informações do usuário local na página 105
Criando usuários locais na página 107
Excluindo um usuário local na página 108
Ativando ou desativando usuários locais na página 109
Alterando as senhas do usuário na página 109
Alterando opções de log-in na página 110

Excluindo um usuário local

Você pode excluir certos usuários com base em sua função de usuário. Se um dos usuários selecionados não puder ser excluído, o botão **Delete** ficará desabilitado. Por exemplo, sysadmin não pode ser excluído.

Etapas

1. Na guia Local Users, selecione um nome de usuário na lista.
2. Clique em **Delete** para excluir as contas de usuário.

3. Na caixa de diálogo Delete User, clique em **Apply** para salvar as alterações.

Conceitos relacionados

Funções de usuário na página 106

Tarefas relacionadas

Visualizando informações do usuário local na página 105
Criando usuários locais na página 107
Modificando um perfil de usuário local na página 108
Ativando ou desativando usuários locais na página 109
Alterando as senhas do usuário na página 109
Alterando opções de log-in na página 110

Ativando ou desativando usuários locais

Você pode habilitar ou desabilitar usuários locais.

Etapas

1. Na guia Local Users, selecione um ou mais nomes de usuário na lista.
2. Selecione o botão **Enable** ou **Disable**.
3. Na caixa de diálogo Enable User or Disable User, clique em **Apply** para salvar as alterações.

Conceitos relacionados

Funções de usuário na página 106

Tarefas relacionadas

Visualizando informações do usuário local na página 105
Criando usuários locais na página 107
Modificando um perfil de usuário local na página 108
Excluindo um usuário local na página 108
Alterando as senhas do usuário na página 109
Alterando opções de log-in na página 110

Alterando as senhas do usuário

A caixa de diálogo Change Password permite que você altere a senha de um usuário selecionado.

Etapas

1. Na guia Local Users, selecione um nome de usuário na lista.
2. Selecione **Change Password**.
3. Na caixa de diálogo Change Password, digite a nova senha na caixa New Password. (Se solicitado, digite a senha antiga também.)
4. Digite a nova senha novamente na caixa Verify New Password.
5. Clique em **Apply** para salvar as alterações.

Conceitos relacionados

Funções de usuário na página 106

Tarefas relacionadas

Visualizando informações do usuário local na página 105
Criando usuários locais na página 107
Modificando um perfil de usuário local na página 108

Excluindo um usuário local na página 108
Ativando ou desativando usuários locais na página 109
Alterando opções de log-in na página 110

Alterando opções de log-in

Você pode modificar as configurações de composição de senhas, o tempo para alterar senhas, limitar tentativas de log-in etc.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Local Users** > **Manage Password Policies**.
2. Na caixa de diálogo Manage Password Policies, digite as informações da política de senha.

Tabela 31. Políticas de senha

Item	Descrição
Minimum Days Between Change	Número mínimo de dias entre as alterações de senha, que deve ser menor que o (Número máximo de dias entre as alterações de senha menos o Número de dias de aviso antes que a senha expire). O padrão é 0.
Maximum Days Between Change	O número máximo de dias entre alterações de senha. O padrão é 90.
Warn Days Before Expire	Número de dias de aviso a um usuário antes que a senha expire, que deve ser menor que o (Número máximo de dias entre alterações de senha menos Número mínimo de dias entre alterações de senha). O padrão é 7.
Disable Days After Expire	O número de dias após a expiração de uma senha para desabilitar a conta de um usuário. Você pode digitar never ou um número > ou igual a 0. O padrão é Never.
Comprimento mínimo da senha	O comprimento mínimo de senha exigido. O padrão é 9. Pode ser definido como um valor de 9 a 31.
Número mínimo de classes de caracteres	O número mínimo de classes de caracteres exigidas. O padrão é 4 e não é configurável. As classes de caracteres incluem e devem ter pelo menos: • Um caractere minúsculo (a-z) • Um caractere maiúsculo (A-Z) • Um caractere numérico (0-9) • Um caractere especial ($, %, #, + e assim por diante)
Requisito de caracteres minúsculos	Habilite ou desabilite o requisito de pelo menos um caractere minúsculo. O padrão é desabilitado.
Requisito de caracteres maiúsculos	Habilite ou desabilite o requisito de pelo menos um caractere maiúsculo. O padrão é desabilitado.
Mínimo de caracteres numéricos	Habilite ou desabilite o requisito de pelo menos um caractere numérico. O padrão é desabilitado.
Mínimo de caracteres especiais	Habilite ou desabilite o requisito de pelo menos um caractere especial. O padrão é desabilitado.
Requisito máximo de caracteres consecutivos	Habilite ou desabilite o requisito de no máximo três caracteres repetidos. O padrão está ativado.
Impor o histórico de reutilização de senha	Especifique o número de senhas memorizadas. A faixa é de 0 a 24. O padrão é 6.
Máximo de tentativas de log-in	Especifique o número máximo de tentativas de log-in antes que um bloqueio obrigatório seja aplicado a uma conta de usuário. Esse limite se aplica a todas as contas de usuário, inclusive sysadmin. Um usuário bloqueado não pode fazer log-in enquanto a conta estiver bloqueada. A faixa é de 4 a 20. O padrão é 4.
Desbloquear timeout (segundos)	Especifique por quanto tempo uma conta de usuário ficará bloqueada após o número máximo de tentativas de log-in. Quando o timeout de desbloqueio configurado for atingido, o usuário poderá tentar fazer log-in novamente. A faixa é de 120 a 3600 segundos. O padrão é 120 segundos.

3. Clique em **Apply** para salvar as alterações.

Conceitos relacionados

Funções de usuário na página 106

Tarefas relacionadas

Visualizando informações do usuário local na página 105
Criando usuários locais na página 107
Modificando um perfil de usuário local na página 108
Excluindo um usuário local na página 108
Ativando ou desativando usuários locais na página 109
Alterando as senhas do usuário na página 109

Usuários ativos

Usuários ativos são aqueles que estão atualmente registrados no DDMC.

Visualizando usuários ativos

Você pode visualizar uma variedade de informações sobre os usuários que estão atualmente conectados ao DDMC.

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Active Users**.
2. Visualize a lista de usuários ativos exibidos.

Tabela 32. Usuários ativos

Item	description
Nome	Nome de usuário com uma sessão ativa
Ociosa	Período desde a última atividade do usuário
Last Login From	Sistema ao qual o usuário fez log-in
Last Login Time	Selo com a data de quando o usuário fez log-in
Terminal	Nota do terminal para log-in da CLI ou *GUI* se o usuário estiver conectado usando a GUI

Configurando a autenticação

O DDMC permite que você configure três tipos de autenticação: Active Directory, Workgroup e NIS.

Autenticação NIS

Contas de usuários locais em um sistema Data Domain ou PowerProtect começam com um ID exclusivo de 500. Ao configurar um sistema em um ambiente de NIS (serviço de informação da rede), considere os conflitos de ID exclusivo em potencial entre as contas de usuário local e de NIS. Para evitar esses conflitos, durante o planejamento inicial, considere o tamanho de contas locais em potencial ao definir faixas de ID exclusivo permitidas para usuários de NIS.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **NIS**.
3. Na área NIS Authentication, visualize informações sobre servidores NIS e grupos de NIS configurados, conforme descrito na tabela a seguir.

Tabela 33. Informações de autenticação do NIS

Item	descrição
NIS Status	Status do serviço: ativado ou desativado
Nome de domínio	Nome do domínio para esse serviço
Servidor	Nome do servidor que executa a autenticação
NIS Group	Nome do grupo de NIS
Management Role	Função de gerenciamento atribuída ao grupo (admin ou usuário)

4. Você pode adicionar, editar ou excluir qualquer uma dessas informações, selecionando o controle apropriado.

Habilitando a autenticação NIS

O domínio do NIS (serviço de informação de rede) mantém um repositório centralizado de usuários, grupos e nomes de servidor. O NIS adiciona um diretório global que autentica os usuários em qualquer host na rede.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **NIS**.
3. Na área **Status**, selecione **Enabled**.
4. Selecione **Apply**.

Desativando a autenticação NIS

Após ativar a autenticação NIS, talvez seja preciso desativá-la ocasionalmente.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **NIS**.
3. Na área **Status**, selecione **Disabled**.
4. Selecione **Apply**.

Configurando os nomes de domínio do NIS

Se um nome de domínio do NIS for inválido, pode levar muito tempo para processar. Lembre-se de digitar um nome de domínio válido.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **NIS**.
3. Digite o novo nome do domínio na caixa de texto Domain Name.
4. Clique em **Apply**.

Configurando servidores NIS

Você pode configurar manualmente os servidores NIS ou pode obtê-los pelo DHCP. Ao configurá-los manualmente, você pode adicionar, modificar ou excluir servidores.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **NIS**.
3. Na área Servidores NIS, selecione **Manual**.

4. Para adicionar um servidor, clique em Add (sinal de mais verde) e especifique um nome.
5. Para excluir um servidor, selecione-o e clique em Delete (X vermelho).
6. Selecione **Apply**.

Configurando grupos de NIS

Você pode adicionar, modificar ou excluir grupos de NIS.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **NIS**.
3. Para adicionar um grupo, clique em Add (sinal de mais verde). Digite um nome, selecione uma função de gerenciamento (admin, limited-admin ou user) e clique em **Add**.
4. Para modificar um grupo, selecione-o e clique em Modify (lápis). Edite o nome e/ou função de gerenciamento (admin ou user) e clique em **Save**.
5. Para excluir um grupo, selecione-o e clique em Delete (X).
6. Clique em **Apply**.

Autenticação do Windows

A autenticação do Windows pode ser configurada usando grupos de trabalho ou o Active Directory.

1. Clique no botão Settings (ícone de engrenagem, no canto superior direito) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **Windows**.
3. Selecione **Using Workgroup** ou **Using Active Directory** na lista drop-down **Method**.

   Para a autenticação de grupo de trabalho, veja as informações sobre os servidores CIFS e grupos de trabalho configurados, conforme descrito na tabela a seguir.

Tabela 34. Informações de servidores CIFS e grupo de trabalho configurado

Item	Descrição
Nome do grupo de trabalho	Nome do grupo de trabalho no qual a instância do DDMC reside.
servidor CIFS	Nome do servidor CIFS onde o DDMC está conectado.

Para a autenticação do Active Directory, veja as informações sobre o Active Directory, conforme descritas na tabela a seguir.

Tabela 35. Informações sobre o Active Directory

Item	Descrição
Nome do realm	Nome do realm do Active Directory.
Nome de usuário	Nome do usuário do Active Directory.
Senha	Senha do Active Directory.
servidor CIFS	Nome do servidor CIFS onde o DDMC está conectado.
Controlador do domínio	Controlador de domínio do Active Directory ao qual o DDMC está conectado.
Unidade organizacional	Nome da unidade organizacional na qual a instância do DDMC reside.
Grupo do Windows	Nome do grupo do Windows no qual a instância do DDMC reside.

Configurando a autenticação do grupo de trabalho

O modo Workgroup associa o DDMC a um domínio de grupo de trabalho.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **Windows**.
3. Selecione **Using Workgroup**.
4. Para Nome do grupo de trabalho, selecione *Manual* para digitar um nome diferente para o grupo de trabalho na caixa de texto.
5. Em CIFS Server Name, selecione *Manual* para digitar um nome diferente do servidor CIFS (sistema Data Domain ou PowerProtect) na caixa de texto.
6. Clique em **Apply**.

Autenticação do Active Directory

Se o Active Directory estiver configurado, você pode usar o painel Active Directory/ Authentication para exibir informações associadas.

Etapas

Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.

NOTA: O nome de usuário e senha são sempre exigidos para aplicar as alterações.

Configurando a autenticação do Active Directory

O DDMC deve cumprir com todos os requisitos do Active Directory, como ter um horário no relógio que não difira mais de 5 minutos do horário do controlador de domínio.

Etapas

Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.

Digitando as credenciais e nome do Realm

Um KDC (Key Distribution Center) do Windows exige as credenciais e o nome do Realm para a autenticação do Active Directory.

Etapas

1. Na caixa de texto Realm Name, digite o nome completo do realm do DDMC, como **`domain1.local`**.
2. Na caixa de texto User Name, digite um nome de usuário. Esse usuário pode estar em um domínio a ser associado ou em um domínio que seja um domínio confiável de sua empresa. O usuário deve ter permissão para criar contas neste domínio. O nome do usuário deve ser compatível com os requisitos da Microsoft para o domínio do Active Directory a ser associado.
3. Na caixa de texto Password, digite uma senha. A senha deve ser compatível com os requisitos da Microsoft para o domínio do Active Directory a ser associado.

Definindo as configurações avançadas do Active Directory

Opcionalmente, você pode definir as configurações avançadas do Active Directory para o nome do servidor CIFS, controladores de domínio e unidade organizacional.

Etapas

1. Para o nome do servidor CIFS:
   - Selecione *Use default: xxx* para usar o nome padrão do servidor CIFS ou
   - Selecione *Manual* e digite o nome do servidor CIFS na caixa de texto.
2. Para Controladores de domínio:
   - Selecione *Atribuir automaticamente*, que é o padrão e o método recomendado ou
   - Selecione *Manual* e digite o(s) nome(s) do controlador nas caixas de texto. Podem ser adicionados até três nomes de controladores. Você pode digitar nomes de domínio completos, nomes de host ou endereços IP (IPv4 ou IPv6).
3. Para unidades organizacionais:
   - Selecione *Use default: xxx* para usar as unidades de organização padrão ou
   - Selecione *Manual* e digite o nome da unidade organizacional na caixa de texto.

NOTA: A conta é movida para a nova unidade organizacional.

4. Selecione **OK**.

Próximas etapas

Depois de configurar a autenticação do Windows, você deve habilitar a autenticação do CIFS na linha de comando do DDMC:

```
adminaccess authentication add cifs
```

Criando grupos do Windows

Um grupo do Windows é um grupo (baseado em uma das funções do usuário: admin ou user) que existe em um controlador de domínio Windows.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **Windows**.
3. Selecione **Using Active Directory**.
4. Clique em **Add**.
5. Especifique um grupo do Windows.
6. Especifique uma função.
7. Clique em **Add**.
8. Clique em **Apply**.

Modificando grupos do Windows

Depois de criar um grupo do Windows, você pode modificá-lo, conforme necessário.

Etapas

1. Selecione **Administration** > **Settings** > **Access tab** > **Authentication**.
2. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
3. Clique na guia **Windows**.
4. Selecione **Using Active Directory**.
5. Selecione um grupo do Windows e clique em **Edit**.
6. Edite o nome do grupo na caixa de texto. O domínio do grupo deve ser especificado, por exemplo, domínio\nome do grupo.
7. Clique em **Save**.
8. Clique em **Apply**.

Excluindo grupos do Windows

Não é possível excluir os grupos padrão do Windows, como administradores de domínio. Se um grupo padrão do Windows for selecionado, o botão Delete ficará esmaecido.

Etapas

1. Selecione **Administration** > **Settings** > **Access tab** > **Authentication**.
2. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
3. Clique na guia **Windows**.
4. Selecione **Using Active Directory**.
5. Selecione um grupo do Windows e clique em **Delete**.
6. Clique em **Apply**.

Autenticação LDAP

O LDAP (Lightweight Directory Access Protocol) pode ser usado para autenticar usuários com acesso ao DDMC. Os usuários do LDAP podem gerenciar os sistemas Data Domain.

Sobre esta tarefa

NOTA: Se você ativar o status do LDAP, o status do NIS será desativado se estiver ativado. Se você ativar o status do NIS, o status do LDAP será desativado se estiver ativado.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **LDAP**.
3. Na área LDAP Authentication, você poderá visualizar informações sobre os servidores LDAP e grupos LDAP configurados, conforme descrito na tabela a seguir.

Tabela 36. Informações sobre a autenticação LDAP

Item	Descrição
Status	Status do serviço: ativado ou desativado
Base suffix	Ponto a partir do qual o servidor pesquisa usuários
Bind DN	Localização do usuário na árvore de diretórios LDAP
Vincular senha	Senha de acesso ao DN vinculado
SSL	Status: ativado ou desativado **NOTA:** Se o SSL estiver desativado, não será possível editar os campos **Protocols** e **Demand server certificate**.
Protocolos	Protocolo SSL: LDAPS ou StartTLS
Demand server certificate	Status: ativado ou desativado
Servidor LDAP	Nome do servidor que executa a autenticação
LDAP group	Nome do grupo LDAP
Função	Função de gerenciamento atribuída ao grupo (administrador ou usuário)

4. Você pode adicionar, editar ou excluir qualquer uma dessas informações, basta selecionar o controle apropriado.

Ativando a autenticação LDAP

O servidor LDAP

Sobre esta tarefa

NOTA: Se você ativar o status do LDAP, o status do NIS será desativado se estiver ativado. Se você ativar o status do NIS, o status do LDAP será desativado se estiver ativado.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **LDAP**.
3. Na área **Status**, selecione **Enabled**.
4. Selecione **Apply**.

Desativando a autenticação LDAP

Após a ativação da autenticação LDAP, poderão surgir situações em que ela precisará ser desativada.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **NIS**.
3. Na área **Status**, selecione **Disabled**.
4. Selecione **Apply**.

Configurando o sufixo de base do LDAP

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **LDAP**.
3. Digite o sufixo de base na caixa de texto.
4. Clique em **Apply**.

Configurando o DN vinculado do LDAP

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **LDAP**.
3. Digite o DN vinculado na caixa de texto.
4. Clique em **Apply**.

Configurando um servidor LDAP

Você pode configurar os servidores LDAP manualmente ou pode obtê-los pelo DHCP (Dynamic Host Configuration Protocol, protocolo de configuração de host dinâmico). Ao configurá-los manualmente, você pode adicionar, modificar ou excluir servidores.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.
2. Clique na guia **LDAP**.
3. Para adicionar um servidor, clique em **Add** (sinal de mais verde) e digite um nome.
4. Para excluir um servidor, selecione-o e clique em **Delete** (X vermelho).
5. Selecione **Apply**.

Configurando grupos LDAP

Adicione, modifique ou exclua grupos LDAP.

Sobre esta tarefa

- Os grupos LDAP são exibidos na lista de usuários da página de permissão de edição.
- Um usuário LDAP de um grupo LDAP configurado pode acessar o DDMC como o NIS ou um usuário do AD.
- Os usuários LDAP vinculados a um grupo LDAP configurado podem visualizar o DD System Manager.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **Access** > **Authentication**.

2. Clique na guia **LDAP**.
3. Para adicionar um grupo, clique em Add (sinal de mais verde). Digite um nome, selecione uma função de gerenciamento (admin, limited-admin ou user) e clique em **Add**.
4. Para modificar um grupo, selecione-o e clique em **Edit** (lápis). Edite o nome e/ou função de gerenciamento (admin, limited-admin ou user) e clique em **Save**.
5. Para excluir um grupo, selecione-o e clique em **Delete** (X).
6. Clique em **Apply**.

Gerenciando definições de configuração geral

Ao acessar as configurações pelo ícone de engrenagem no banner do DDMC, você pode gerenciar configurações do servidor de e-mail, o modo como data e hora são obtidos e algumas propriedades do sistema (local, e-mail padrão do administrador e nome do host).

Configurando definições de data e hora

Você pode definir ou alterar as configurações do fuso horário e como o horário do sistema é sincronizado (não sincronizado ou com o NTP (Network Time Protocol)).

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **Time and Data**.
2. Defina como o horário será sincronizado:
   - Para definir manualmente a data e a hora, selecione **Manual**, digite a data na caixa de texto e use as listas drop-down para definir a hora.
   - Para usar o NTP a fim de sincronizar a hora, selecione **NTP** e escolha como acessar o servidor NTP.
     - **Obtain NTP Servers using DHCP** — o DHCP selecionará automaticamente um servidor.
     - **Manually Configure** — adicione o endereço IP do servidor na área **NTP Servers**.
3. Selecione **Apply**.

   NOTA: As modificações nas configurações de **Time and Dete** exigem uma reinicialização do DDMC para entrarem em vigor.

Conceitos relacionados

Trabalhando com o SNMP na página 93

Tarefas relacionadas

Definindo configurações do servidor de e-mail na página 119
Configurando propriedades do sistema na página 118

Configurando propriedades do sistema

Você pode fornecer um endereço de e-mail de administrador para ser adicionado às listas de notificação de alerta e autosupport, além de um host de administrador para ser adicionado às listas de acesso FTP e Telnet, usando a página de configuração Properties, em Settings Lightbox.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **Properties**.
2. O campo de texto Location mostra onde o sistema está localizado. [Esse campo de texto não é usado pelo DDMC (ou DD OS); ele está aqui simplesmente para sua informação.]
3. Na seção Default Administrator, digite um endereço de e-mail para ser adicionado automaticamente às listas de notificação de alerta e autosupport, além de um host para ser adicionado automaticamente às listas de acesso do FTP e Telnet. Digitar ALL nesse campo dá permissão a todos os hosts para o FTP e Telnet.
4. Clique em **Apply**.

Conceitos relacionados

Trabalhando com o SNMP na página 93

Tarefas relacionadas

Definindo configurações do servidor de e-mail na página 119
Configurando definições de data e hora na página 118

Definindo configurações do servidor de e-mail

Você pode definir ou alterar o nome de seu servidor de e-mail usando a caixa de diálogo Set Mail Server.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **Properties**.
2. Digite o nome do servidor de e-mail na caixa de texto.
3. Clique em **Apply**.

Conceitos relacionados

Trabalhando com o SNMP na página 93

Tarefas relacionadas

Configurando definições de data e hora na página 118
Configurando propriedades do sistema na página 118

Verificar um número de série do DDMC

Cada máquina virtual do DDMC possui um número de série exclusivo, que é usado para identificar o sistema em mensagens do autosupport.

NOTA: Números de série não podem ser adicionados ou alterados. Eles são atribuídos automaticamente.

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **Properties**.
2. Visualize o número de série registrado.

NOTA: O DDMC não exige uma licença, mas os sistemas Data Domain e PowerProtect gerenciados devem ter licenças para seus recursos principais e opcionais.

Gerenciando alertas

Você pode definir as configurações para determinar quem receberá as notificações de alerta do DDMC e os resumos de alertas diários.

O DDMC e o DD OS usam o mesmo sistema de alerta. Informações detalhadas sobre o sistema de alerta estão descritas no *DD OS Administration Guide*.

Gerenciando notificações de alerta

Os grupos que estão configurados para receber notificações de alerta do DDMC estão listados na **Settings** > **System** > **Support** > **Notifications** guia. A seleção de um grupo na tabela preenche os painéis Detalhes para os atributos de classe do alerta e de assinantes que recebem notificação quando os alertas atingem a severidade que está configurada para a classe do alerta.

Criando um grupo de notificação

Por padrão, todos os alertas são enviados ao grupo de e-mail autosupport-alert@autosupport.datadomain.com, mas outros grupos podem ser criados para receber classes específicas de notificações de alertas.

Etapas

1. Clique no botão **Settings** (o ícone de engrenagem) no banner do DDMC e, em seguida, selecione **System** > **Support** > **Notifications**.
2. Na área Real Time Alerts, clique em **Add**.
3. Na caixa de diálogo Add Notification Group, digite um nome para o grupo na caixa de texto Group Name.
4. Selecione os atributos de classe de alerta e defina o nível de severidade no qual as notificações serão enviadas.
   Por exemplo, você pode criar um grupo CriticalWarnings, selecionar todas as classes e definir o nível de severidade para Critical.
5. No painel Subscribers, clique em Add (sinal de mais verde), adicione o endereço de e-mail de um assinante.
6. Repita essa etapa para cada assinante que precise ser adicionado ao grupo e clique em **Add**.

Verificando e-mails de assinantes em um grupo de notificação

Você pode enviar um e-mail de teste para assinantes em um grupo de notificação a fim de verificar se os endereços de e-mail estão em funcionamento.

Etapas

1. No menu **More Tasks**, selecione **Send Test Alert**.
2. No painel Notification Groups, selecione as linhas dos grupos que devem receber o e-mail de teste e, em seguida, selecione **Next**.
3. No painel Additional Email Addresses, adicione ou modifique os endereços de e-mail, se necessário.
4. Selecione **Send Now**.

Modificando um grupo de notificação

Você pode modificar vários aspectos de um grupo de notificação.

Etapas

1. Clique na linha do grupo na tabela de grupos Notifications e selecione **Modify**.
2. Na caixa de diálogo Modify Group, selecione **Group Properties** e na área Class Attributes, adicione ou remova classes, altere os níveis de severidade e selecione **Next**.
3. A área Assinantes é exibida. Adicione ou remova endereços de e-mail de assinantes, conforme necessário e selecione **Next**.

Excluindo um grupo de notificação

Você pode excluir qualquer grupo de notificação, exceto o grupo de notificação padrão.

Etapas

1. Marque uma ou mais linhas de grupos na tabela de grupo Notifications e selecione **Delete**.
2. Na caixa de diálogo Delete Group, verifique a exclusão e selecione **OK**.
3. Selecione **OK** para sair da caixa de diálogo de confirmação.

Redefinindo um grupo de notificação

Você pode remover todos os grupos de notificação que foram adicionados e remover quaisquer alterações feitas no grupo padrão.

Etapas

1. No menu **More Tasks**, selecione **Reset Notification Groups**.
2. Na caixa de diálogo Reset Notification Groups, clique em **Yes** e na caixa de diálogo Verification, selecione **OK**.

Gerenciando uma lista de assinantes

É possível adicionar, modificar ou excluir endereços de e-mail em uma lista de assinantes do grupo de notificação.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **Support** > **Notifications**.
2. Selecione o grupo de notificação desejado e clique em **Edit**.
3. Na caixa de diálogo Edit Subscribers, selecione umas das seguintes opções:
   - Para adicionar um assinante, clique em Add (sinal de mais verde). Digite o endereço de e-mail na caixa de diálogo Email Address e clique em **Add**.
   - Para modificar um endereço de e-mail, selecione-o na lista Subscriber Email e clique em Modify (lápis). Edite o endereço de e-mail na caixa de diálogo Email Address e clique em **Save**.
   - Para excluir um endereço de e-mail, selecione-o na lista Subscriber Email e clique em Delete (X).
4. Clique em **Apply**.

Gerenciando os resumos de alertas diários

Todas as manhãs, às 8h, horário local do DD Management Center, um e-mail de resumo de alertas diários, que contém os resumos de alertas e mensagens de registro, é enviado aos assinantes configurados.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **Support** > **Notifications**.
2. Se o horário de envio padrão "8:00 AM Daily" não for aceitável, selecione a hora, minuto e AM/PM para obter uma nova hora.
3. Gerencie os e-mails para assinantes:
   - Para adicionar um assinante, clique em Add (sinal de mais verde). Digite o endereço de e-mail na caixa de diálogo Email Address e clique em **Add**.
   - Para modificar um endereço de e-mail, selecione-o na lista Subscriber Email e clique em Modify (lápis). Edite o endereço de e-mail na caixa de diálogo Email Address e clique em **Save**.
   - Para excluir um endereço de e-mail, selecione-o na lista Subscriber Email e clique em Delete (X).
4. Clique em **Apply**.

Gerenciando a geração de relatórios do autosupport

O recurso de geração de relatórios do autosupport envia por e-mail um relatório diário gerado automaticamente, chamado de ASUP, para o suporte da Dell EMC.

Esse relatório mostra a identificação do sistema DDMC, as informações de status e as entradas de vários arquivos de log. Informações e estatísticas internas amplas e detalhadas estão incluídas no final do relatório para ajudar a equipe de suporte com a depuração, se necessário. No entanto, não há nenhuma informação sobre sistemas gerenciados neste relatório.

A geração de relatórios do Autosupport fica habilitada por padrão. Para desabilitá-la:

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **Support** > **DELL EMC SUPPORT**.
2. Desmarque a opção **Auto support and daily alert summary** e/ou **Real-time alert**.
3. Clique em **Apply**.

NOTA: Para obter informações adicionais sobre a geração de relatórios automática de suporte, consulte o *DD OS Administration Guide*.

Como usar o Dell EMC Secure Remote Services ou e-mail preexistente para suporte automático

Por padrão, os relatórios de autosupport são ativados e enviados diariamente para o atendimento ao cliente da Dell EMC usando o *método de e-mail preexistente*. O *Dell EMC Secure Remote Services* envia mensagens com segurança por meio de um gateway do Secure Remote Service.

Sobre esta tarefa

Para determinar se a geração de relatórios de autosupport está habilitada no momento, e em caso afirmativo, o método de uso é:

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **Support** > **DELL EMC SUPPORT**.
2. Na área Channel, selecione **Dell EMC Secure Remote Services**.
3. Adicione, exclua ou altere as prioridades do método.

   Para alterar o método, consulte o *Guia de administração do DD OS*.
4. Selecione a frequência para enviar o e-mail para o administrador padrão do DDMC.
5. Clique em **Apply**.

Adicionando à lista de e-mail do relatório do autosupport

Por padrão, os relatórios de autosupport são ativados e enviados diariamente para o Atendimento ao cliente da Dell EMC. Você pode desejar adicionar endereços de e-mail adicionais como destinatários de relatórios de autosupport.

Etapas

1. Clique no botão **Settings** (o ícone de engrenagem) no banner do DDMC e, em seguida, selecione **System** > **Support** > **Notifications**.
2. Na seção Autosupport Report, selecione Add (sinal + verde) para adicionar um endereço de e-mail.
3. Clique em **Apply**.

Analisando relatórios gerados pelo autosupport

O painel de relatórios do autosupport contém uma lista de links para os arquivos atuais de relatórios do autosupport.

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **Support** > **REPORT HISTORY**.
2. Para consultar um relatório gerado pelo autosupport, selecione o link de um nome do arquivo e visualize o relatório usando um editor de texto. Se seu navegador exigir, faça download do arquivo primeiro.

Gerando um pacote de suporte manualmente

Durante a solução de problemas, o Suporte da Dell EMC pode solicitar que você gere imediatamente um pacote de suporte, que é uma seleção de arquivos de registro com compactação tar-g e um arquivo LEIA-ME que inclui a identificação de cabeçalhos de autosupport.

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **Support** > **Support Bundles**.
2. Clique em **Generate Support Bundles**.
3. Quando você visualizar o novo arquivo .tar.gz, envie-o por e-mail ao suporte do Data Domain. Se ele for grande demais para ser enviado por e-mail, acesse o site de suporte da Dell EMC e faça upload dele.

Gerenciando logs do sistema

Um arquivo de mensagens e o arquivo de log de auditoria são salvos no DDMC e listados na área Logs. Os arquivos podem ser abertos e salvos localmente e depois encaminhados para o suporte, se necessário.

Etapas

1. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **Support** > **Logs**.
2. Na página Logs, visualize o nome do arquivo de log (que é atribuído automaticamente), o tamanho do arquivo e a data em que ele foi modificado pela última vez. Selecione o nome de um arquivo de log para visualizar seu conteúdo. Você pode ser solicitado a selecionar um aplicativo, como Notepad.exe, para abrir o arquivo.
3. Salve o arquivo de log no local, se necessário.

Atualizando o software DDMC

Somente os administradores do DDMC têm permissão para gerenciar os pacotes de atualização de software e realizar atualizações do DDMC.

Você pode fazer a atualização diretamente para o DDMC 7.7 em um sistema que esteja executando o DDMC 6.2 ou posterior. Para fazer atualização do DDMC 7.7 a partir de uma família de versões anterior à 6.2, será preciso fazer atualização em etapas.

Tabela 37. Atualização direta

Versão do DDMC	Atualização direta para:
7.6	7.7
7.5	7.6 e 7.7
7.4	7.5, 7.6 e 7.7
7.3	7.4, 7.5, 7.6 e 7.7
7.2	7.3, 7.4, 7.5, 7.6 e 7.7
7.1	7.2, 7.3, 7.4, 7.5, 7.6 e 7.7
7.0	7.1, 7.2, 7.3, 7.4, 7.5, 7.6 e 7.7
6.2	7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6 e 7.7
6.1	6.2, 7.0, 7.1, 7.2, 7.3 , 7.4 e 7.5
2.0	6.1 e 6.2
1.4.5	2.0 e 6.1
1.3	1.4, 1.4.5 e 2.0
1.2	1.3 e 1.4
1.1	1.2 e 1.3

NOTA: A família de versões do DDMC imediatamente seguinte à 2.0 é a 6.1; não existem as versões 3.x, 4.x ou 5.x.

NOTA: A família de versão do DDMC diretamente depois de 6.2 é 7.0.

A atualização do software do DDMC é realizada em duas etapas:

- Obtendo uma imagem do site de suporte on-line ou selecionando uma imagem de atualização obtida anteriormente que esteja salva.
- Fazendo atualização no DDMC.

O DDMC 7.7 é compatível com o gerenciamento de sistemas que executam até oito versões anteriores (DDOS 7.6, 7.5, 7.4, 7.3, 7.2, 7.1, 7.0 e 6.2) e a próxima versão quando estiver disponível.

Gerenciar pacotes de atualização do DDMC

Você pode fazer download de uma imagem de atualização no site de suporte on-line para uma unidade acessível localmente e, em seguida, adicioná-la ao conjunto de pacotes de atualização gerenciado pelo DDMC.

Etapas

1. Use o ícone de engrenagem **Settings** no banner do DDMC. **Sistema**. Os usuários admin e limited-admin podem acessar a opção **Support Bundles**.
2. Na área Pacotes de Atualização, visualize os pacotes de atualização disponíveis, seus tamanhos e datas de modificação. Depois, selecione uma das seguintes opções:
   - Para obter um novo pacote de atualização para armazenar localmente, clique em **Add**.
   - Para fazer upload de um pacote que foi armazenado localmente no inventário, clique em **Add**e depois no link **Dell EMC Online Support** Navegue até a unidade local para selecionar o pacote.
   - Para excluir um pacote, selecione-o na lista de inventário e clique em **Delete**.
3. Para realizar a atualização, consulte o procedimento na seção a seguir.

Pré-requisito para executar uma atualização de software do DDMC

Um terceiro disco com 100 GB (usando vCenter/vSphere Client) deve ser adicionado antes de atualizar para o DDMC 7.6.

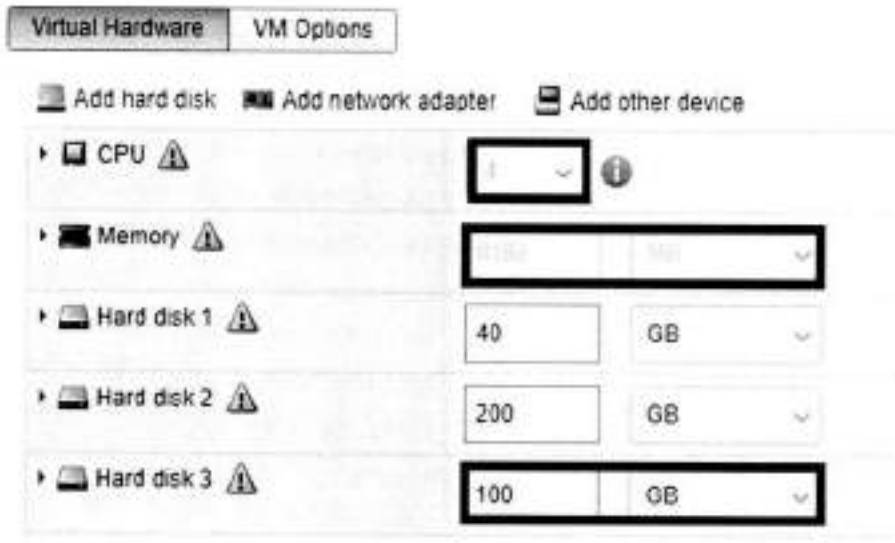


Figura 6. Adicione o terceiro disco com 100 GB

Os arquivos de atualização de software usam a extensão `.rpm`. Este tópico assume que a atualização é só do DDMC. Caso você faça alterações no hardware, como adicionar, trocar ou mover placas de interface, é preciso atualizar as configurações do DDOS para corresponder às alterações.

Atualização do software DDMC no ESXi

Etapas

1. Analise as Notas da versão do DDMC apropriadas para obter instruções sobre essa atualização e para verificar o espaço disponível.

   NOTA: Na maior parte das versões, são permitidas atualizações de até duas versões anteriores.

2. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **UPDATE**.
3. Na área Update Packages Available, selecione o pacote de atualização na lista e depois **Perform System Update**.
4. Monitore o progresso da atualização na página do console do DDMC.
5. Esteja ciente de que o processo de atualização reinicializa automaticamente o DDMC.
6. É recomendado que você mantenha aberta a caixa de diálogo de progresso de System Update até que a atualização seja concluída ou que o sistema seja desligado.

Como realizar uma atualização de software do DDMC na KVM

Após fazer o upload de um pacote de atualização, você pode usá-lo para atualizar o software DDMC.

Pré-requisitos

Um terceiro disco com 100 GB deve ser adicionado antes da atualização para o DDMC 7.6.

1. Crie um arquivo de disco virtual de 100 GB.

```
Create Virtual Disk : root@test:/data# qemu-img create -f raw /data/ddmc-yang-db-3rd-disk 100G
```

2. Listar máquinas virtuais, selecionar e verificar as configurações.

```
root@CNBJDPDKVM01:~/ddmc-kvm-7.4.0.5-671629# virsh list
Id Name State
```

```
----------------------------------------------------
1 ddmc-676052 running
3 ddmc-yang-671629 running
```

3. Adicione o novo arquivo de disco criado no arquivo de configuração da máquina virtual. Salve e saia.

```
root@CNBJDPDKVM01:/kvm-root/images# virsh attach-disk ddmc-7.1.0.40-663551-wanj4 --source /
kvm-root/images/ddmc-7.1.0.40-663551-wanj4-svc --target sdc --persistent
Disco conectado com sucesso
```

Sobre esta tarefa

NOTA: Os arquivos de atualização de software usam a extensão `.rpm`. Este tópico assume que a atualização é só do DDMC. Caso você faça alterações no hardware, como adicionar, trocar ou mover placas de interface, é preciso atualizar as configurações do DDOS para corresponder às alterações.

Etapas

1. Analise as Notas da versão do DDMC apropriadas para obter instruções sobre essa atualização e para verificar o espeço disponível.

   NOTA: Na maior parte das versões, são permitidas atualizações de até duas versões anteriores.

2. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **UPDATE**.
3. Na área Update Packages Available, selecione o pacote de atualização na lista e depois **Perform System Update**.
4. Monitore o progresso da atualização na página do console do DDMC.
5. O processo de atualização reinicia automaticamente o DDMC.
6. É recomendado que você mantenha aberta a caixa de diálogo de progresso de System Upgrade até que o upgrade seja concluído ou que o sistema seja desligado.

Como realizar uma atualização de software do DDMC no Hyper-V

Após fazer o upload de um pacote de atualização, você pode usá-lo para atualizar o software DDMC.

Pré-requisitos

Um terceiro disco com 100 GB (usando o gerenciador Hyper-V) deve ser adicionado antes de atualizar para o DDMC 7.6.

1. Clique no menu de configuração da máquina virtual.
2. Clique no botão **Add** para adicionar um novo disco rígido.
3. Use o **assistente de novo disco rígido virtual**.
4. O novo disco adicionado deve ser de 100 GB.
5. Adicionar o disco.

Sobre esta tarefa

NOTA: Os arquivos de atualização de software usam a extensão `.rpm`. Este tópico assume que a atualização é só do DDMC. Caso você faça alterações no hardware, como adicionar, trocar ou mover placas de interface, é preciso atualizar as configurações do DDOS para corresponder às alterações.

Etapas

1. Analise as Notas da versão do DDMC apropriadas para obter instruções sobre essa atualização e para verificar o espaço disponível.

   NOTA: Na maior parte das versões, são permitidas atualizações de até duas versões anteriores.

2. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **UPDATE**.
3. Na área Update Packages Available, selecione o pacote de atualização na lista e depois **Perform System Update**.
4. Monitore o progresso da atualização na página do console do DDMC.
5. O processo de atualização reinicia automaticamente o DDMC.
6. É recomendado que você mantenha aberta a caixa de diálogo de progresso de System Upgrade até que o upgrade seja concluído ou que o sistema seja desligado.

Como realizar uma atualização de software do DDMC na AWS

Após fazer o upload de um pacote de atualização, você pode usá-lo para atualizar o software DDMC.

Pré-requisitos

Um terceiro disco de 100 GB deve ser adicionado antes de atualizar para o DDMC 7.6.

1. Abra o console da Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. Na barra de navegação, selecione a região em que o DDMC está localizado.
3. No painel de navegação, selecione **Elastic Block Store** > **Volumes**.
4. Clique em **Create Volume**.
   - Volume Type: escolha um tipo de volume igual a disco raiz ou disco de banco de dados.
   - Tamanho: 100 GB
   - Availability Zone: escolha a zona de disponibilidade na qual deseja criar o volume. (Um volume EBS deve ser conectado a uma instância do EC2 que esteja na mesma zona de disponibilidade que o volume.)
   - Deixe os valores padrão para os outros campos.
   - Clique em Add Tag, Key: Name, Value: Forneça a string que identifica este terceiro disco de serviço.
   - Clique em **Create Volume**

Conecte o terceiro disco a uma instância.

1. Abra o console da Amazon EC2 em https://console.aws.amazon.com/ec2/.
2. No painel de navegação, selecione **Elastic Block Store**.
3. Selecione um volume disponível e selecione **Actions** > **Attach Volume**.
4. Para **Instance**, comece a digitar o nome ou o ID da instância. Selecione a instância na lista de opções (somente as instâncias que estiverem na mesma zona de disponibilidade que o volume serão exibidas).
5. Para **Device**, você pode manter o nome do dispositivo sugerido ou digitar um nome de dispositivo compatível diferente. Para obter mais informações, consulte Nomear dispositivos em instâncias do Linux.
6. Selecione **Attach**.

Para o 7.6, o tipo de instância deve ser m4.xlarge ou m5.xlarge. Se o tipo de instância não corresponder, um alerta será exibido. A recomendação é usar o m5.xlarge.

Execute as etapas a seguir para redimensionar a instância do DDMC se o tipo de instância atual não for m5.xlarge.

1. Abra o console do Amazon EC2 e, no painel de navegação, selecione **Instances**.
2. Selecione a instância do DDMC e clique em **Actions** > **Instance state** > **Stop instance**.
3. Na caixa de diálogo **Stop Instance**, clique em **Stop**.

   NOTA: Pode demorar alguns minutos até que a instância pare.
4. Assim que a instância do DDMC estiver no estado parado, acesse **Actions** > **Instance settings** > **Change instance type**.

   NOTA: Essa ação não estará disponível se o estado da instância não estiver parado.
5. Na caixa de diálogo **Change instance type**, selecione o tipo de instância e clique em **Apply**.
6. Acesse **Instance state** > **Start instance** para iniciar a instância.

   NOTA: Pode demorar alguns minutos para a instância entrar no estado de execução.

Sobre esta tarefa

NOTA: Os arquivos de atualização de software usam a extensão `.rpm`. Este tópico assume que a atualização é só do DDMC. Caso você faça alterações no hardware, como adicionar, trocar ou mover placas de interface, é preciso atualizar as configurações do DDOS para corresponder às alterações.

Etapas

1. Analise as Notas da versão do DDMC apropriadas para obter instruções sobre essa atualização e para verificar o espaço disponível.

   NOTA: Na maior parte das versões, são permitidas atualizações de até duas versões anteriores.
2. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **UPDATE**.
3. Na área Update Packages Available, selecione o pacote de atualização na lista e depois **Perform System Update**.
4. Monitore o progresso da atualização na página do console do DDMC.

5. O processo de atualização reinicia automaticamente o DDMC.
6. É recomendado que você mantenha aberta a caixa de diálogo de progresso de System Update até que a atualização seja concluída ou que o sistema seja desligado.

Como modificar o atributo da instância do DDMC para adicionar o adaptador de rede elástico (ENA)

Se a instância do DDMC foi implementada manualmente, o atributo de instância do DDMC deve ser modificado para adicionar o suporte ao adaptador de rede elástico (ENA) antes de alterar o tipo de instância para m5.xlarge.

Etapas

1. Use o comando da CLI da AWS a seguir para verificar se a instância atual do DDMC tem suporte a ENA.
   Neste exemplo, `i-0bddc2cc1c9f9d61c` é o ID da instância do DDMC. Use o ID da instância do DDMC específico ao executar esse comando. Se o resultado for `[]` com conteúdo vago, isso significa que a instância atual do DDMC não é compatível com o ENA.

   ```
   $  aws ec2 describe-instances --instance-ids i-0bddc2cc1c9f9d61c --query
   "Reservations[].Instances[].EnaSupport"
   []
   ```
2. Use o comando da CLI da AWS a seguir para adicionar o atributo de suporte ENA para sua instância do DDMC.

   ```
   $ aws ec2 modify-instance-attribute --instance-id i-0bddc2cc1c9f9d61c  --ena-support
   ```
3. Depois de executar o comando acima, use o seguinte comando da CLI da AWS para verificar se o atributo de suporte do ENA está em vigor ou não. Se o resultado é `true` , a instância do DDMC deve ter o atributo de suporte a ENA e você pode alterar o tipo de instância para m5.xlarge.

   ```
   $  aws ec2 describe-instances --instance-ids i-0bddc2cc1c9f9d61c --query
   "Reservations[].Instances[].EnaSupport"
   [
       true
   ]
   $
   ```
4. Abra o console do Amazon EC2 e, no painel de navegação, selecione **Instances**.
5. Selecione a instância do DDMC, clique em **Instance state** e, em seguida, clique em **Stop instance**.
6. Na caixa de diálogo **Stop instance**, clique em **Stop**.
   Pode demorar alguns minutos até que a instância do DDMC pare.
7. Assim que a instância do DDMC estiver no estado Parado, na barra de navegação, clique em **Actions** > **Instance settings** > **Change instance type**.
8. Na caixa de diálogo **Change instance type**, selecione **m5.xlarge instance type**, clique em **Apply** .
9. Selecione a instância do DDMC e clique em **Instance state** > **Start instance**.
   Pode demorar alguns minutos até que a instância do DDMC entre no estado de execução.

Como realizar uma atualização de software do DDMC no Azure

Após fazer o upload de um pacote de atualização, você pode usá-lo para atualizar o software DDMC.

Pré-requisitos

Um terceiro disco com 100 GB deve ser adicionado antes do upgrade para o DDMC 7.6.

1. Acesse o portal do Azure: https://portal.azure.com.
2. Nos serviços do Azure, clique em **Virtual Machine**.
3. Selecione e clique na instância do DDMC.
4. Nas configurações, clique em **Disks**.
5. Clique em **Create** e acople um novo disco.
   - Disk name: digite a string de nome para o terceiro disco de serviço.
   - Storage type: escolha o tipo do mesmo que o disco raiz ou o disco de banco de dados.
   - Tamanho: 100 GB
   - Host caching: None

- Clique em **Save**.

O tipo de instância D4s_v3 é obrigatório. Se o tipo de instância não corresponder, um alerta será exibido.

1. Clique em Virtual instance.
2. Selecione e clique na instância do DDMC.
3. Em Settings, clique em **Size**.
4. Pesquise e selecione **D4s_v3**.
5. Clique em **Resize**.

Sobre esta tarefa

Etapas

1. Analise as Notas da versão do DDMC apropriadas para obter instruções sobre essa atualização e para verificar o espaço disponível.

   NOTA: Na maior parte das versões, são permitidas atualizações de até duas versões anteriores.

2. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **UPDATE**.
3. Na área Update Packages Available, selecione o pacote de atualização na lista e depois **Perform System Update**.
4. Monitore o progresso da atualização na página do console do DDMC.
5. O processo de atualização reinicia automaticamente o DDMC.
6. É recomendado que você mantenha aberta a caixa de diálogo de progresso de System Upgrade até que o upgrade seja concluído ou que o sistema seja desligado.

Como realizar uma atualização de software do DDMC na GCP

Após fazer o upload de um pacote de atualização, você pode usá-lo para atualizar o software DDMC.

Pré-requisitos

Um terceiro disco com 100 GB deve ser adicionado antes do upgrade para o DDMC 7.6.

1. Acesse o console do GCP: https://console.cloud.google.com/.
2. Clique em **Compute Engine**, **VM instances**, e selecione a instância do DDMC.
3. Clique em **Edit** em Discos adicionais e clique em **Add new disk**.
   - Name: digite a string de nome para o terceiro disco de serviço
   - Type: defina-o como o mesmo tipo de disco raiz ou de banco de dados
   - Tamanho: 100 GB
4. Clique em **Save**.

O tipo de instância e2-standard-4 é obrigatório. Se o tipo de instância não corresponder, um alerta será exibido.

1. Acesse o console do GCP: https://console.cloud.google.com/
2. Clique em **Compute Engine**, **VM instances**, e selecione a instância do DDMC.
3. Na barra de navegação, clique em STOP para interromper a instância do DDMC.
4. Depois que a instância do DDMC estiver no estado interrompido, clique em EDIT na barra de navegação
5. Na configuração da máquina:
   - **Machine family** > **General-purpose** > **Series**: Selecione **select E2**
   - **Machine Type**: selecione **e2-standard-4**
6. Clique em **Save**.

Sobre esta tarefa

Etapas

1. Analise as Notas da versão do DDMC apropriadas para obter instruções sobre essa atualização e para verificar o espaço disponível.

   NOTA: Na maior parte das versões, são permitidas atualizações de até duas versões anteriores.

2. Clique no botão **Settings** (ícone de engrenagem) no banner do DDMC e selecione **System** > **UPDATE**.

3. Na área Update Packages Available, selecione o pacote de atualização na lista e depois **Perform System Update**.
4. Monitore o progresso da atualização na página do console do DDMC.
5. O processo de atualização reinicia automaticamente o DDMC.
6. É recomendado que você mantenha aberta a caixa de diálogo de progresso de System Upgrade até que o upgrade seja concluído ou que o sistema seja desligado.

A

Referência gráfica para o DDMC

Tópicos:

- Ícones e controles globais
- Controles de Painel de Controle
- Controles de recursos
- Ícones de grupo
- Controles de propriedade

Ícones e controles globais

Os controles e ícones usados na interface do DDMC são descritos em detalhes.

Tabela 38. Controles que executam uma função

Controle	Nome	Descrição
	Alerts	Localizado no banner do DDMC, mostra os alertas mais recentes; um ponto vermelho notifica sobre alertas ativos não vistos
	Help	Localizado no banner do DDMC, e um menu suspenso é exibido quando clicado: • Sobre o DD Management Center • O que há de novo • Visualizar EULA • Guia do DDMC: é proveniente do *Guia de Instalação e Administração do PowerProtect DD Management Center*
	Usuário	Um ícone circular é exibido com a primeira letra alfabética do ID do usuário. Localizado no banner do DDMC e é usado para: • Exibir informações de usuário e função • Alternar para o modo de exibição clássico • Log-out
	Configurações	Localizado no banner do DDMC e oferece acesso direto às configurações de rede, acesso e sistema
	Atualizar	Localizado no banner do DDMC, recarrega a página para exibir informações mais recentes
	Controles de filtro	O controle de filtro é composto por duas partes: o ícone do funil e uma lista drop-down. • Se a filtragem estiver sendo executada, clicar no funil desativará toda a filtragem, fazendo com que todos os sistemas fiquem visíveis. • Se o filtro estiver desativado, clicar no funil ativará a filtragem, usando o filtro definido anteriormente. • Quando um filtro estiver ativo, a exibição do funil fica amarela. Selecione **Show Filter** ou o link **Filtered by** para ver os detalhes sobre o que é filtrado. A seleção de filtro é realizada com a pequena seta para baixo, que abre uma lista drop-down dos tipos de filtragem que podem ser empregados para: • **Filter by group** — permite a seleção de um ou mais grupos. Sistemas que pertencem aos grupos selecionados são exibidos no painel do ambiente de trabalho.

Tabela 38. Controles que executam uma função (continuação)

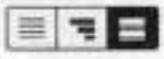
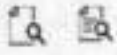
Controle	Nome	Descrição
		• **Filter by property** — permite a seleção de um ou mais valores de propriedade. Os sistemas que possuem esses valores de propriedade são exibidos no painel do ambiente de trabalho. • **Filter by property** — permite a seleção de um ou mais sistemas para serem exibidos no painel do ambiente de trabalho. • **Filter by rule** — permite a criação de uma regra do filtro (ou a seleção de uma regra criada anteriormente) que controla quais sistemas são exibidos no painel do ambiente de trabalho. Filtrar por regra é usado para combinar sistemas, grupos e propriedades para alcançar maior granularidade. **NOTA:** Você deve alternar para o modo de exibição clássico para usar o recurso **Filter by rule**. • A filtragem é usada no painel do ambiente de trabalho para exibições de monitoramento, mas não para recursos de relatórios e de painel de controle.
•  • 	Alternância de visualização de sistema ou de grupo	• **View by System** (padrão) — exibe os sistemas como uma lista simples, cujas entradas são classificáveis usando os controles de classificação de colunas da tabela. • **View by Group** — exibe sistemas por sua hierarquia de grupo. Nessa exibição, a classificação de tabela é realizada somente dentro de grupos. As listas de grupo podem ser expandidas para uma lista de sistemas.
	Alternância de exibição de sistema, grupo, tenant	Igual ao ícone anterior, mas você também pode selecionar: • **View by Tenant** — exibe os tenants como uma lista simples, cujas entradas são classificáveis usando controles de classificação de coluna da tabela.
	Visualizar o DD System Manager	Inicia o DD System Manager para o sistema selecionado, na qual você pode gerenciar ou investigar diretamente a área correspondente de onde ele foi iniciado.
	Detalhes do inventário	Encontrado na guia **Infrastructure** > **UpdateSystems** na coluna **Details**. O ícone alterna entre ocultar e exibir as alternações.
	Mostrar colunas	Encontrado em muitas das visualizações que são baseadas em tabela, permite a escolha das colunas que são exibidas na tabela.
	Classificação da coluna	Em visualizações de tabela, classifica a exibição das colunas em ordem crescente ou decrescente (por data, em ordem alfabética, por prioridade etc), com base no tipo de dados da coluna.
	Adicionar	Abre uma caixa de diálogo para adicionar um ou mais itens. O tipo de item que está sendo adicionado depende da página exibida. Por exemplo, na página **Inventory** > **Systems**, isso permite que você adicione sistemas ao DDMC. Na página **Administration** > **Properties**, isso permite que você crie propriedades personalizadas para os objetos gerenciados.
	Editar	Para um elemento selecionado da tabela, será aberta uma caixa de diálogo que permite alterar as informações sobre o elemento.
	Excluir	Exclui um elemento selecionado da tabela.
	Continuar	Continua uma operação, como a adição de outra instrução ao criar uma regra personalizada.

Tabela 39. Ícones que mostram o status do sistema e/ou conexão

Ícone	Status
	Normal — a comunicação entre o DDMC e o sistema DD está funcionando normalmente.
	Unreachable — o sistema não está respondendo ou não está transmitindo. Os dados foram recuperados pela última vez na data exibida no banner de status.

Tabela 39. Ícones que mostram o status do sistema e/ou conexão (continuação)

Ícone	Status
	Unmanaged — o sistema está suspenso ou não é gerenciado. Quando suspenso, toda a coleta de dados será interrompida. O sistema será suspenso se o gerenciamento tiver sido realizado por outro DDMC ou quando o sistema for suspenso usando a CLI.
	Adding — o sistema está sendo adicionado ao inventário.
	Upgrading — o sistema está sendo atualizado e fica indisponível durante esse estado.
	Synchronizing — os dados do sistema estão sendo sincronizados. O sistema fica indisponível durante esse estado.
	Unsupported system — esse sistema não é compatível porque ele está executando um sistema operacional que não é compatível com esta versão do DDMC. Você pode exibir os detalhes do sistema, mas os dados estarão desatualizados. Você verá uma dica de ferramenta com a opção de atualizar o sistema.

Tabela 40. Ícones para tenants e unidades de tenant

Ícone	Status
	Tenant Unit Configuration Issues — reportado em todas as páginas de multi-tenancy, caixas de diálogo e lightboxes, indica que essa unidade de tenant não possui lista de notificação de alerta configurada, nenhum armazenamento provisionado, nenhum conjunto de cota fixa e/ou nenhum relatório configurado.

Tarefas relacionadas

Trabalhando com filtros na página 40
Fazer log-in no DDMC na página 23

Controles de Painel de Controle

A página **Dashboard** > **Monitoring** consiste em uma a sete guias que você cria para conter qualquer número de recursos que ofereçam exibições de monitoramento rápidas e de alto nível de vários aspectos do ambiente do Data Domain ou PowerProtect.

Tabela 41. Controles de Painel de Controle

Controles	Nome	Descrição
+	Adicionar painel de controle/guia	A caixa de diálogo **Add Dashboard** é aberta
	Adicionar recurso	Abre a caixa de diálogo **Add Dashboard Widget**, na qual é possível selecionar um modelo de recurso e filtros opcionais para criar um recurso.
	Adicionar/configurar guias	Abre a caixa de diálogo **Add and Configure Dashboard Tabs**, na qual é possível adicionar guias, modificar nomes de guias ou excluir guias. Também é possível definir o número de colunas e alterar a ordem das guias no painel de controle.
	Maximizar/restaurar o painel de controle	Alterna o tamanho do painel de controle. **Maximize** oculta o painel de navegação e **Restore** retorna ao modo de exibição padrão, exibindo o painel de navegação.

Tarefas relacionadas

Trabalhando com filtros na página 40

Controles de recursos

Cada recurso inclui os controles padrão a seguir.

Tabela 42. Controles de recursos

Controles	Nome	Descrição
	Editar recurso	Abre o recurso Edit Dashboard, em que você pode alterar o nome e os critérios de filtro do recurso e, em alguns casos, os detalhes do recurso.
	Detalhes	O botão global de aprofundamento sobre um recurso que navega para a página mãe associada ao recurso. Por exemplo, para os recursos Alerts, a página **Health** > **Alerts** é aberta.
	Help	Apresenta informações sobre o que o recurso monitora e sobre os controles ativos no recurso, como o controle para navegar até a página de monitoramento pai.
	Remover recursos	Exclui o recurso da guia.
 Status	Connection Status	Clique em **Status** para abrir um pop-up que lista as contagens dos sistemas com problemas de conexão em qualquer uma dessas categorias: (não respondendo, não transmitindo, suspenso e não gerenciado). Inclui um link na parte inferior do pop-up para navegar para a página **Health** > **Status** que fornece mais detalhes sobre estes sistemas. **NOTA:** O controle **Status** é exibido em um recurso quando qualquer um dos sistemas monitorados (filtrados ou não filtrados) tem um ou mais problemas de conexão.
	Filtro de tabela inativo/ativo	Indica que um filtro está inativo ou ativo em uma coluna da tabela em que a filtragem está disponível.
	Filtro	Indica que um filtro está ativo para o recurso.
	Emergência e alerta	Quando um estado de emergência ou alerta estiver presente, clique nesse ícone para abrir a página **Status** > **Alerts** para mostrar as mensagens de alerta/emergência.
	Crítico e erro	Quando estados críticos ou de erro estiverem presentes, clique nesse ícone para abrir a página **Status** > **Alerts** para mostrar as mensagens de crítico/erro.
	Advertência	Quando existir uma advertência, clique nesse ícone para abrir a página **Status** > **Alerts** para mostrar a advertência.

Ícones de grupo

Na página **Administration** > **Groups**, o administrador do sistema DDMC cria grupos em uma hierarquia de árvore para organizar de maneira lógica os sistemas Data Domain e PowerProtect.

Tabela 43. Ícones de grupo

Controles	Nome	Descrição
	Grupo	Simboliza um grupo que contém sistemas ou outros grupos. Quando subgrupos estiverem presentes, o ícone do expansor é exibido à esquerda da pasta. A seleção da pasta exibe os membros do grupo no painel de detalhes do grupo.
	Grupo com permissões aplicadas	Indica que esse grupo é controlado por permissões de acesso.
	Detalhes da lista de membros	É exibido quando um sistema pertencer a mais de um grupo. Passe o mouse para visualizar os nomes dos grupos dos quais esse sistema é um membro.

Controles de propriedade

Os controles usados para adicionar, editar e atribuir propriedades (**Administration** > **Properties**) ajudam a ver rapidamente se uma propriedade é de sistema ou de usuário e ajudam a obter mais detalhes e informações sobre a propriedade.

Tabela 44. Controles de propriedade

controles	nome	descrição
	Propriedade do sistema	Denota uma propriedade fixa e predefinida que não pode ser editada. A seleção desse controle mostra todos os seus valores criados na coluna Valores. As propriedades padrão, que não podem ser modificadas, são: • System — Model, OS, Domain Name • MTrees — Replicated • Replication — sem propriedades padrão
	Propriedade do usuário	Denota uma propriedade definida pelo usuário. Quando selecionada, pode ser editada ou excluída e todos os seus valores criados são exibidos na coluna Valores.
	Detalhes do sistema	Abre a caixa de diálogo de Property Assignment, que lista o tipo de propriedade, o nome do elemento (por exemplo, nome do sistema) e o valor atribuído. Quando aberta na coluna Valores, mostra apenas as entidades para esse valor.

B

Interface de linha de comando do DDMC

Tópicos:

- Diferenças entre a CLI do DDMC e a CLI do DDOS
- Tarefas disponíveis somente na CLI do DDMC
- Comandos config template
- comandos managed-system
- comandos de tarefas

Diferenças entre a CLI do DDMC e a CLI do DDOS

A CLI (interface de linha de comando) do DD é derivada da CLI do DDOS, mas foi modificada para atender às necessidades e tarefas do DD.

- Há dois comandos exclusivos do DDMC (`managed-system` e `task`) que executam registro, administração e funções de gerenciamento de trabalho básicos.
- Apenas um subconjunto (quinze) dos comandos do DDOS (`adminaccess`, `alerts`, `alias`, `authentication`, `autosupport`, `config`, `help`, `log`, `net`, `ntp`, `route`, `snmp`, `support`, `system`, `user`) está incluído no DDMC; no entanto, alguns argumentos e resultados não estão incluídos porque o DDMC não gerencia o armazenamento diretamente. Os comandos restantes do DDOS não estão incluídos porque eles estão preocupados apenas com o gerenciamento de armazenamento.

Para consultar a ajuda on-line para um comando da CLI no DDMC, inicie uma sessão de shell seguro (SSH) e digite ? no prompt da CLI ou digite `man` *Command-Name*.

Tarefas disponíveis somente na CLI do DDMC

É recomendável que você use a GUI do DDMC para todas as tarefas de gerenciamento do sistema. No entanto, você deve usar a CLI do DDMC para algumas tarefas de administração do sistema que não estão disponíveis na GUI.

- `managed-system resume` *host*
- `managed-system suspend` *host*
- `managed-system sync`
- `system show performance` [duration *duration* {hr | min}] [interval *interval* [hr | min]]
- `system show serialno detailed`

  A GUI mostra o número de série atual do DDMC, mas não é compatível com a versão detalhada.

- `system show space`
- `system show stats` [view {net | lostat | sysstat}] [custom-view *view-spec,...*] [interval *nsecs*] [count *count*]

Comandos config template

Esforços de configuração de sistemas Data Domain e PowerProtect com configuração idêntica ou muito semelhante agora podem ser minimizados pelo uso do conjunto `config template` de comandos da CLI para configuração de grupos de sistemas.

config template apply

Esse comando aplica um modelo de configuração a sistemas de proteção selecionados que o DDMC gerencia.
`config template apply` *template-name* `to-managed-systems` *host-list*

NOTA: *host-list* é uma lista de nomes de host gerenciados pelo DDMC; endereços IP numéricos não são permitidos.

config template create

Esse comando cria um modelo de configuração a partir de um sistema de proteção e o salva no banco de dados local no DDMC.
`config template create template-name from-managed-system host-name features | all | adminaccess | alerts | autosupport | config | net | ntp | snmp | feature-list | [description template-description ]`

NOTA: Apenas um nome de host é permitido.

Tabela 45. Recursos e subrecursos do `config template`

Recurso	Sub-recursos	Operação
Adminaccess	ssh	Habilitar/Desabilitar
	hosts ssh	Adicionar/Excluir
	scp	Habilitar/Desabilitar
	telnet	Habilitar/Desabilitar
	hosts telnet	Adicionar/Excluir
	ftp	Habilitar/Desabilitar
	hosts ftp	Adicionar/excluir
	ftps	Habilitar/Desabilitar
	http	Habilitar/Desabilitar
	host http	Adicionar/Excluir
	https	Habilitar/Desabilitar
	web-service	Habilitar/Desabilitar
	porta http de opção Web	Definir/Redefinir
	Porta https de opção Web	Definir/Redefinir
	timeout de sessão da opção Web	Definir/Redefinir
Alertas	grupo da lista de notificação	Criar/excluir
	e-mails da lista de notificação	Adicionar/Excluir
	severidade de classe da lista de notificação	Adicionar/Excluir
Autosupport	resumo do alerta	Adicionar/Excluir
	e-mails de resumo do alerta	Adicionar/Excluir
	detalhado por asup	Adicionar/Excluir
	e-mails detalhados por asup	Adicionar/Excluir
Config	host admin	Definir/Redefinir
	e-mail do admin	Definir/Redefinir
	servidor de e-mail	Definir/Redefinir
	timezone	Definir/Redefinir
Net	interface	Habilitar(ativado)/Desabilitar(desativado)
	dhcp	Sim/Não
	hosts	Adicionar/Excluir
	dns	Definir/Redefinir
NTP	servidor de horário	Adicionar/Excluir

Tabela 45. Recursos e subrecursos do `config template` (continuação)

Recurso	Sub-recursos	Operação
	status	Habilitar/Desabilitar
SNMP (Simple Network Management Protocol)	status	Habilitar/Desabilitar
	Contato do sistema	Definir/Redefinir
	Local do sistema	Definir/Redefinir
	ro-community	Adicionar/Excluir
	ro-community hosts	Adicionar/Excluir
	rw-community	Adicionar/Excluir
	rw-community hosts	Adicionar/Excluir
	trap-host	Adicionar/Excluir
	user	Adicionar/Excluir

config template creation schedule set

Esse comando pode ser usado para configurar um agendamento diário para criar modelos de configuração em para todos os sistemas de proteção gerenciados pelo DDMC.

- São salvas no máximo 3 cópias (criadas pelo agendador) por sistema de proteção.
- Se nenhuma configuração for alterada do dia anterior, não é feita cópia

```
config template creation schedule set { hh:mm | never }
```

config template creation schedule reset

Esse comando redefine um agendamento diário para interromper a criação de modelos de configuração para todos os sistemas de proteção gerenciados pelo DDMC.

```
config template creation schedule reset
```

config template destroy

Esse comando destrói um modelo de configuração salvo no banco de dados local no DDMC.

```
config template destroy template-name
```

config template rename

Esse comando renomeia um modelo de configuração do DDMC já existente.

```
config template rename template-name new-template-name
```

config template show detailed

Esse comando exibe as configurações detalhadas de um modelo de configuração disponível para uso dos sistemas de proteção que são gerenciados pelo DDMC.

```
config template show detailed [template-name]
```

config template show list

Esse comando exibe uma lista de modelos configurados disponíveis para uso dos sistemas de proteção gerenciados pelo DDMC.

```
config template show list [template-name]
```

comandos managed-system

Os comandos da CLI `managed-system` do DDMC permitem que você adicione e remova sistemas do gerenciamento, altere suas configurações de host do proxy e suspenda, retome ou sincronize a coleta de dados.

NOTA: Você também pode usar a interface Web para realizar essas ações.

managed-system add

```
managed-system add hostname [force] [inbound-proxy proxy-host [inbound-proxy-port proxy-port]]
[outbound-proxy proxy-host [outbound-proxy-port proxy-port]]
```

Esse comando adiciona um sistema ao conjunto de sistemas gerenciados. O comando solicita que você:

1. Verifique se o certificado obtido do host é válido.
2. Digite a senha do sysadmin para o sistema que está sendo adicionado ao gerenciamento.

Definições de argumento

force	Se o sistema já estiver sendo gerenciado por outro DD Management Center, o DD Management Center atual assume o gerenciamento do sistema Data Domain do outro DD Management Center e o entrada do sistema Data Domain deste outro DD Management Center é colocada no estado Unmanaged. Se o sistema já estiver sendo gerenciado e esse argumento for omitido, o comando falhará.
hostname	O nome do host do sistema.
inbound-proxy *proxy-host*	Nome do host do proxy de entrada se a conexão de entrada do sistema Data Domain for feita por um proxy.
inbound-proxy-port *proxy-port*	Número da porta de entrada do proxy se a conexão de entrada do sistema Data Domain for feita por um proxy.
outbound-proxy *proxy-host*	Nome do host do proxy de saída se a conexão do DD Management Center ao sistema Data Domain for feita por um proxy.
outbound-proxy-port *proxy-port*	Número da porta de saída do proxy se a conexão do DD Management Center ao sistema Data Domain for feita por um proxy.

NOTA: As opções de proxy são equivalentes às opções de firewall na GUI.

managed-system check-connection

```
managed-system check-connection hostname [inbound-proxy proxy-host [inbound-proxy-port proxy-
port]] [outbound-proxy proxy-host [outbound-proxy-port proxy-port]]
```

Esse comando verifica se o host especificado está acessível e disponível para ser gerenciado por este DDMC. Use `managed-system add` para adicionar o sistema ao conjunto de sistemas gerenciados por este DDMC.

Definições de argumento

hostname	O nome do host do sistema.
inbound-proxy *proxy-host*	Nome do host do proxy de entrada se a conexão de entrada do sistema Data Domain for feita por um proxy.
inbound-proxy-port *proxy-port*	Número da porta de entrada do proxy se a conexão de entrada do sistema Data Domain for feita por um proxy.
outbound-proxy *proxy-host*	Nome do host do proxy de saída se a conexão do DD Management Center ao sistema Data Domain for feita por um proxy.

outbound-proxy-port *proxy-port*	Número da porta de saída do proxy se a conexão do DD Management Center ao sistema Data Domain for feita por um proxy.

managed-system delete

`managed-system delete hostname`

Esse comando remove o sistema especificado do gerenciamento do DDMC.

Definições de argumento

hostname	O nome do host do sistema.

managed-system resume

`managed-system resume hostname`

Esse comando retoma a coleta de dados do sistema DD especificado se a coleta tiver sido suspendida por `managed-system suspend`.

NOTA: Se um sistema estiver executando uma versão incompatível do DD OS, ele será retomado, mas será colocado novamente em estado incompatível (não suspenso).

Definições de argumento

hostname	O nome do host do sistema.

managed-system set

`managed-system set hostname [inbound-proxy {proxy-host|none}] [inbound-proxy-port {proxy-port|default}] [outbound-proxy {proxy-host|none}] [outbound-proxy-port {proxy-port|default}]`

Esse comando define ou altera informações do servidor proxy para um sistema gerenciado.

Definições de argumentos

hostname	O nome do host do sistema.
inbound-proxy {*proxy-host*|none}	Nome do host do proxy de entrada se a conexão de entrada do sistema Data Domain for feita por um proxy. Use `none` para remover o host do proxy e limpar a porta do proxy.
inbound-proxy-port *proxy-port*	Número da porta de entrada do proxy se a conexão de entrada do sistema Data Domain for feita por um proxy.
outbound-proxy {*proxy-host*|none}	Nome do host do proxy de saída se a conexão do DD Management Center ao sistema Data Domain for feita por um proxy. Use `none` para remover o host do proxy e limpar a porta do proxy.
outbound-proxy-port {*proxy-port*|default}	Número da porta de saída do proxy se a conexão do DD Management Center ao sistema Data Domain for feita por um proxy. Use `default` para redefinir o número da porta do proxy.

managed-system show

`managed-system show [{all | hostname}]`

Esse comando imprime informações básicas de uma lista de sistemas gerenciados ou do sistema especificado.

Definições de argumento

all	Gerar relatórios sobre todos os sistemas. Esse é o padrão.
hostname	O nome do host do sistema.

O relatório lista os sistemas por nome de host e inclui o número de série, o estado do gerenciamento, status on-line, versão do DD OS e o tempo da sincronização mais recente.

Estados de gerenciamento

Essa lista descreve os valores possíveis da coluna `State` de gerenciamento.

adicionando	O DDMC está em processo de assumir o gerenciamento do sistema.
excluindo	O DDMC está em processo de finalizar o gerenciamento do sistema.
managed	O DDMC está gerenciando o sistema.
suspenso	O DDMC não está gerenciando e coletando informações sobre o sistema no momento. Os sistemas entram nesse estado se você usar o `managed-system suspend` para interromper a coleta de dados ou se um problema de licenciamento impedir a coleta de dados.
unmanaged	O DDMC gerenciava o sistema anteriormente, mas outro DDMC assumiu o gerenciamento.
unsupported	Esse sistema não é compatível porque sua versão do DD OS não é compatível com esta versão do DDMC.

Valores de status do gerenciamento de sistemas "gerenciados"

Essa lista descreve os possíveis valores de `Status` do gerenciamento quando um sistema está no estado `managed`.

not-responding	O DDMC não foi capaz de enviar mensagens para o sistema gerenciado ou a comunicação apresentou falha em ambas as direções por mais de 30 minutos.
não transmitindo	O sistema gerenciado não respondeu às mensagens do DDMC por mais de 120 minutos.
online	A comunicação com o sistema gerenciado está normal.
upgrading	O sistema gerenciado está em processo de fazer upgrade de seu DD OS.
upgrading, not-responding	O sistema gerenciado está no processo de fazer upgrade de seu DD OS e não está se comunicando com o DDMC.

managed-system suspend

`managed-system suspend hostname`

Esse comando suspende a coleta de dados do host especificado. Se não quiser que o DDMC mostre um sistema como inacessível enquanto ele estiver desligado para manutenção, você pode usar esse comando para suspender o monitoramento.

NOTA: Se um sistema não estiver em um estado gerenciado, ele não poderá ser suspenso. Se um sistema estiver executando uma versão incompatível do DD OS, ele poderá ser suspenso.

Definições de argumento

hostname	O nome do host do sistema.

managed-system sync

`managed-system sync`

Esse comando sincroniza e processa dados atuais e históricos de todos os sistemas gerenciados.

comandos de tarefas

Na CLI, *trabalhos* são chamados de *tarefas*. Os comandos da CLI `task` do DDMC permitem que você cancele, pause, retome e gere relatórios sobre trabalhos. Os usuários regulares podem trabalhar com as tarefas que eles criaram. O usuário sysadmin pode trabalhar em todas as tarefas.

A página **Health** > **Jobs** na interface Web exibe informações sobre os trabalhos que foram iniciados com o DDMC, inclusive os trabalhos ainda em andamento e que foram concluídos ou não com sucesso. Os trabalhos incluem ações como a adição e remoção de sistemas do gerenciamento.

task cancel

`task cancel` *`task-id`*

Esse comando encerra uma tarefa.

Definições de argumentos

task-id	O número de ID da tarefa, conforme relatado por um dos comandos `task show`.

task pause

`task pause` *`task-id`*

Esse comando suspende uma tarefa. Use `task resume` para continuar a tarefa.

Definições de argumentos

task-id	O número de ID da tarefa, conforme relatado por um dos comandos `task show`.

task resume

`task resume` *`task-id`*

Esse comando continua uma tarefa que você suspendeu com `task pause`.

Descrições de argumentos

task-id	O número de ID da tarefa, conforme relatado por um dos comandos `task show`.

task show active

`task show active [type {inventory | replication | upgrade}] [user user]`

Esse comando informa sobre tarefas em execução de nível superior. Você pode filtrar os resultados usando `type` com uma das palavras-chave ou com a palavra-chave `user`.

Definições de argumentos

type {inventory | replication | upgrade}	Filtre os resultados para mostrar somente as tarefas do tipo especificado.

usuário *user*	Filtre os resultados para mostrar somente as tarefas pertencentes ao usuário especificado.

task show detailed

`task show detailed task-id`

Esse comando imprime um relatório detalhado sobre as entradas e saídas de uma tarefa em formato de lista de valores-chave.

Definições de argumento

task-id	O número de ID da tarefa, conforme relatado por um dos comandos `task show`.

task show detailed-active

`task show detailed-active [type {inventory | replication | upgrade}] [user user]`

Esse comando imprime um relatório detalhado sobre as tarefas ativas e suas subtarefas. Você pode filtrar os resultados usando `type` com uma das palavras-chave ou com a palavra-chave user.

Definições de argumentos

type {inventory | replication | upgrade}	Filtre os resultados para mostrar somente as tarefas do tipo especificado.
usuário *user*	Filtre os resultados para mostrar somente as tarefas pertencentes ao usuário especificado.

task show detailed-history

`task show detailed-history [last n {hours | days | weeks | months}] [start MMDDhhmm[[CC]YY] end MMDDhhmm[[CC]YY] [type {inventory | replication | upgrade}] [user user]`

Esse comando imprime um relatório detalhado sobre as tarefas concluídas e suas subtarefas. Você pode filtrar os resultados usando `type` com uma das palavras-chave ou com a palavra-chave `user`. Você pode filtrar os resultados por hora, usando as palavras-chaves `last`, `start` e `end`. O período padrão do relatório são as últimas 24 horas.

Definições de argumentos

last *n* {hours | days | weeks | months}	Filtre os resultados para mostrar somente as tarefas concluídas durante n`hours`, `days`, `weeks` ou `months` anteriores.
start *MMDDhhmm*[[*CC*]*YY*] end *MMDDhhmm*[[*CC*]*YY*]	Filtre os resultados para mostrar somente as tarefas concluídas durante o intervalo especificado. *MMDD* indica mês e dia. *hhmm* indica horas e minutos no formato de 24 horas. Para especificar meia-noite entre domingo à noite e segunda-feira da manhã, use **`mon 0000`**. Para especificar meio-dia na segunda-feira, use **`mon 1200`**. *CC* são os primeiros dois dígitos do ano. *YY* são os dois últimos dígitos do ano.
type {inventory | replication | upgrade}	Filtre os resultados para mostrar somente as tarefas do tipo especificado.
usuário *user*	Filtre os resultados para mostrar somente as tarefas pertencentes ao usuário especificado.

task show history

`task show history [last n {hours | days | weeks | months}] [start MMDDhhmm[[CC]YY] end MMDDhhmm[[CC]YY] [type {inventory | replication | upgrade}] [user user]`

Esse comando imprime um relatório de resumo sobre as tarefas concluídas. Você pode filtrar os resultados usando `type` com uma das palavras-chave ou com a palavra-chave `user`. Você pode filtrar os resultados por hora, usando as palavras-chaves `last`, `start` e `end`. O período padrão do relatório são as últimas 24 horas.

Definições de argumentos

last *n* {hours | days | weeks | months}	Filtre os resultados para mostrar somente as tarefas concluídas durante *n*`hours`, `days`, `weeks` ou `months` anteriores.
start *MMDDhhmm*[[*CC*]*YY*] end *MMDDhhmm*[[*CC*]*YY*]	Filtre os resultados para mostrar somente as tarefas concluídas durante o intervalo especificado. *MMDD* indica mês e dia. *hhmm* indica horas e minutos no formato de 24 horas. Para especificar meia-noite entre domingo à noite e segunda-feira de manhã, use **mon 0000**. Para especificar meio-dia na segunda-feira, use **mon 1200**. *CC* são os primeiros dois dígitos do ano. *YY* são os dois últimos dígitos do ano.
type {inventory | replication | upgrade}	Filtre os resultados para mostrar somente as tarefas do tipo especificado.
usuário *user*	Filtre os resultados para mostrar somente as tarefas pertencentes ao usuário especificado.

CLOUD

Dell EMC PowerProtect DD Seri Appliances with DDOS 7.5

Details on the features and benefits of the latest DDOS release for your PowerProtect DD Series Appli

By David Tye | February 23, 2021

Topics in this article

Data Center

With spring just around the corner, we are pleased to announce the next release of DDOS, version 7.5. powers both the DD and DP series of PowerProtect appliances from Dell Technologies. DDOS provides deliver our high-speed, scalable and industry-leading multi-cloud protection storage for backup, archive

When paired with Dell EMC Data Protection Suite, DD series is the ultimate protection storage applianc Protection Suite go together like peanut butter and jelly. The two together offer a complete data protecti software delivers simple, comprehensive, and flexible data protection. When DD series is coupled with are benefitting from industry leading deduplication and encryption – which optimizes storage and compu encompassing protection solution not only reduces the risks of data loss, it also provides efficiency and cyber recovery demand.

What's new with DDOS 7.5?

DDOS 7.5 includes several enhancements, security updates, and the expansion of our regional covera Edition (DDVE) running in Azure.

When it comes to managing your DD series environment on-prem and in-cloud PowerProtect DD Mana

0:00 / 1:46

Last year, we announced the introduction of DDVE supporting in-cloud instances of up to 256TB fo AW DDOS 7.5, DDVE now has greater regional coverage in the China region when running in Azure.

As with all DDOS releases, we continue our commitment to data security. This latest release includes th crypto-libraries and provides the ability to use two factor authentication (2FA) with RSA SecurID for cert

Last but not least, for customers backing up to a VTL from IBMi, we have added VTL support for LTO-7

You can learn more about the Dell EMC Data Protection Portfolio check out the on-demand content fror If you have any questions about this release, please reach out to your sales representative to learn mor about PowerProtect DD series appliances check us out online. Make sure to follow us on Twitter for the Technologies Data Protection Portfolio

DELL Technologies

White paper técnico

Equipamentos da série Dell EMC PowerProtect DD: compactação assistida por hardware

Resumo geral

Este white paper explica a compactação aprimorada assistida por hardware nos equipamentos Dell EMC PowerProtect série DD DD6900, DD9400 e DD9900

Abrilde 2021

H18734.1

Revisões

Data	Descrição
Junho de 2020	Versão inicial
Abrilde 2021	White paper atualizado com novos detalhes de melhorias de desempenho da série DD

Agradecimentos

Autor: Vinod Kumar Kumaresan

Índice

Resumo executivo

Os equipamentos da série Dell EMC PowerProtect DD reduzem o volume de dados armazenados pelo processo de desduplicação e compactação. Equipamentos da geração anterior compactam dados usando o algoritmo lz padrão. Outros tipos de algoritmos de compactação, como gzfast e gz, também estavam disponíveis. Esses algoritmos ofereciam maior compactação exigindo maior carga da CPU e fornecendo, assim, uma compensação entre desempenho e utilização de espaço.

DD6900, DD9400 e DD9900 estão equipados com compactação assistida por hardware que permite maior compactação usando o gzfast como o algoritmo padrão e sem perder desempenho.

Público

Este white paper técnico destina-se a clientes, parceiros e funcionários da Dell EMC que gostariam de entender a compactação aprimorada assistida por hardware disponível com os equipamentos da série PowerProtect DD.

1 Introdução

1.1 Visão geral da tecnologia

Os equipamentos da série DD têm tecnologia assistida por hardware que oferece maior compactação a um desempenho maior do que os equipamentos da geração anterior. Essa nova tecnologia resulta em aumentos de até 30% na capacidade lógica armazenada e reduz as janelas de backup e restauração dos clientes.

DD9900

- **Largest, fastest PowerProtect DD model**
- **Up to 94TB/hour throughput**
- **Up to 228PB logical capacity support with Dell EMC Cloud Tier**

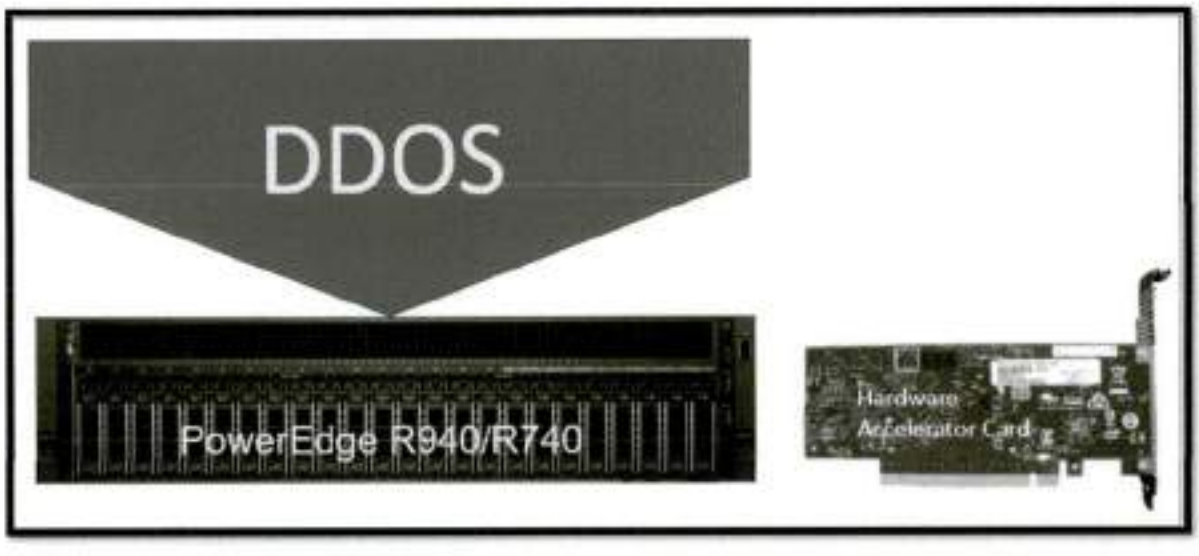
DD9400

- **Up to 57TB/hour throughput**
- **Up to 149.8PB logical capacity support with Dell EMC Cloud Tier**
- **High availability option**

DD6900

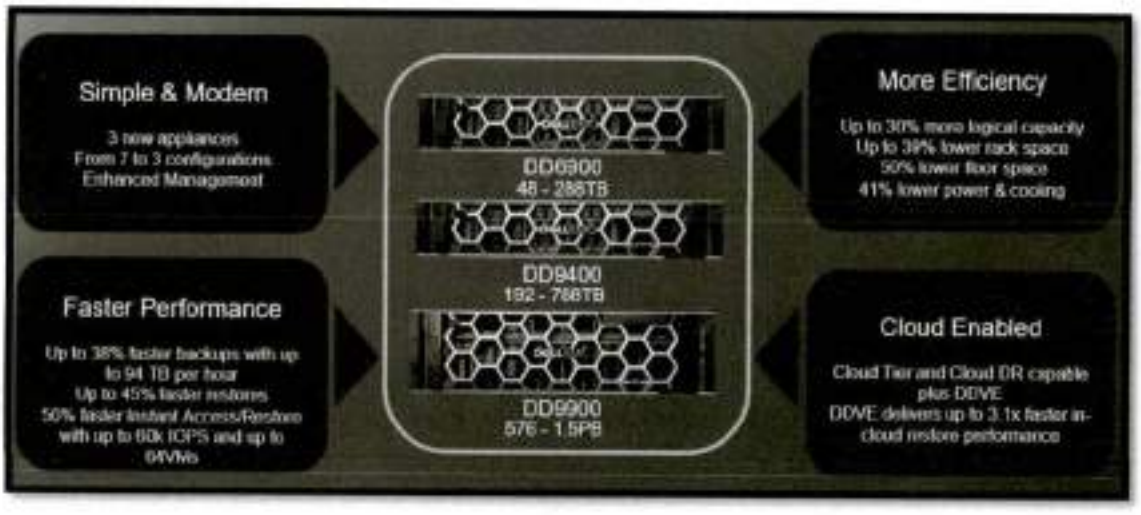
- **Up to 33TB/hour throughput**
- **Up to 56.1PB of logical capacity support with Dell EMC Cloud Tier**
- **High-availability configurations**

Os equipamentos das séries DD6900, DD9400 e DD9900 estão equipados com uma placa aceleradora de hardware usada para compactação.

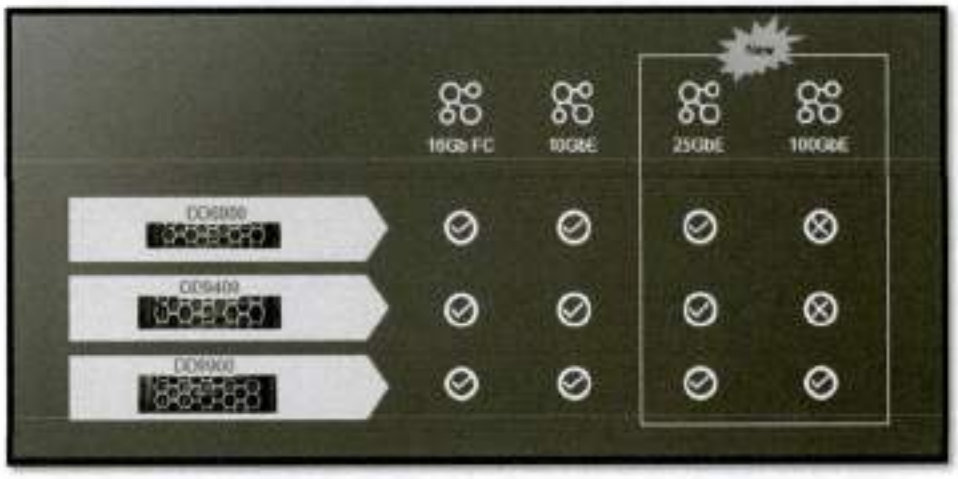


Isso permite que o DDOS deixe os processos de compactação e descompactação para o acelerador de hardware e libere recursos da CPU para melhorar o desempenho do equipamento. O algoritmo de compactação gzfast é o método de compactação local padrão usado em todos os equipamentos DD6900, DD9400 e DD9900. Não há necessidade de configuração adicional. Esse algoritmo gera maior compactação em comparação com a geração anterior do Data Domain, que, por padrão, usa o algoritmo lz. Para ter esse benefício, não é necessário fazer outras configurações.

2 Benefícios



- Até 30% mais capacidade lógica em comparação com equipamentos Data Domain de gerações anteriores
  - ✓ Os equipamentos Data Domain anteriores usam lz como algoritmo de compactação local padrão
  - ✓ DD6900/DD9400/DD9900 usam o gzfast por padrão, oferecendo taxa de compactação até 30% melhor do que o lz em comparação com a geração anterior do Data Domain
- Melhorias de desempenho
  - ✓ Melhora no desempenho de 5% a 25% dependendo da carga de trabalho – restauração, inclusão de NFS/CIFS/VTL
  - ✓ Nenhuma regressão de desempenho para outras cargas de trabalho, inclusão pura do DDBoost, GC e carga de trabalho de replicação
- Uso do produto
  - ✓ Ativado por padrão em todos os equipamentos da série DD – DD6900/DD9400/DD9900
- Série DD: opções de rede mais rápidas
  - ✓ Até 10 vezes o throughput da geração anterior
  - ✓ Permite que mais fluxos de backup sejam agregados com menos conexões de rede



2.1 Portfólio abrangente da série DD

	DD6900	DD9400	DD9900
Max Throughput	Up to 15 TB/hr	Up to 26 TB/hr	Up to 41 TB/hr
Max Throughput (DD Boost)	Up to 33 TB/hr	Up to 57 TB/hr	Up to 94 TB/hr
Logical Capacity[1]	Up to 18.7PB	Up to 49.9PB	Up to 97.5PB
Logical Capacity with Cloud Tier	Up to 56.1PB	Up to 149.8PB	Up to 228PB
Usable Capacity	48TB – 288TB	192TB – 768TB	576TB – 1.5PB
Usable Capacity with Cloud Tier	Up to 864TB	Up to 2.3PB	Up to 3.5PB
ES40 Shelf	4TB 7.2K SAS	8TB 7.2K SAS[3]	8TB 7.2K SAS[3]
DS60 Shelf	4TB 7.2K SAS[3]	8TB 7.2K SAS	8TB 7.2K SAS
FS25 Shelf	3.84TB SSD[2]	3.84TB SSD[2]	3.84TB SSD[2]

2.2 Compactação aprimorada com a série DD

Os dados de telemetria da Dell EMC mostram que os clientes com equipamentos Data Domain que migram para a série DD com compactação assistida por hardware usando o gzfast terão taxas de compactação mais altas em comparação com as gerações anteriores do Data Domain que utilizavam o método de compactação lz. Os dados mostram que a taxa de compactação local aumentará em média 30% para cargas de trabalho que não são de banco de dados e em 31%, 26% para cargas de trabalho MS SQL e Oracle respectivamente. Esses números pressupõem que as cargas de trabalho ainda não estejam pré-compactadas ou criptografadas.

Carga de trabalho	Média de melhoria
Não banco de dados (file system, e-mail etc.)	30%
MS SQL	31%
Oracle	26%

Obs.: os valores de melhoria mencionados na tabela acima são a média observada nas cargas de trabalho do cliente e podem ser revisados no futuro à medida que agregamos mais dados. Os resultados reais podem variar.

3 Compatibilidade

3.1 DDBoost

- Os clientes DDBoost podem continuar operando sem alterações ou impacto no desempenho com os equipamentos da série DD e Data Domain da geração anterior.
- Os clientes DDBoost são transparentes para o processo de compactação na série DD. No entanto, haverá benefícios com as melhorias de desempenho durante o backup e a restauração.

3.2 Replicação

- A replicação entre os equipamentos Data Domain da geração anterior e da série DD continua sendo compatível.
- Não há impacto no desempenho devido aos diferentes algoritmos de compactação usados para equipamentos Data Domain sem compactação assistida por hardware ao replicar para ou da série DD.

3.3 Nível da nuvem

- Os equipamentos da série DD usam a mesma compactação padrão (gzfast) para os dados de retenção em longo prazo na nuvem

3.4 Upgrade do controlador para os equipamentos DD6900/DD9400/DD9900

- Todos os novos dados incluídos são armazenados usando a nova compactação padrão (gzfast) aproveitando a compactação assistida por hardware.
- Todos os dados incluídos anteriormente e armazenados usando a compactação padrão anterior (lz) serão descompactados usando a CPU durante a restauração.
- Todos os dados anteriormente compactados pelo lz serão convertidos em gzfast durante o ciclo de limpeza programado regularmente como parte do processo de recuperação de espaço. Todos os dados compactados no lz precisarão de vários ciclos de limpeza regulares antes de serem totalmente convertidos. Observe que a programação agressiva de ciclos de limpeza não agilizará a conversão, pois a recuperação de espaço pode não ocorrer.
- Todos os dados em camadas usando a compactação padrão anterior permanecerão nesse formato até que o espaço seja recuperado na nuvem. Nenhuma conversão será feita para os dados na nuvem.

4 Hardware da série DD

4.1 Configuração

Nenhum procedimento de configuração manual é necessário.

Equipamento	Número do slot de cartão de assistência de hardware	PCIe LnkSta
DD6900	4	LnkSta: velocidade de 8 GT/s, largura x16
DD9400	4	LnkSta: velocidade de 8 GT/s, largura x16
DD9900	2 e 7	LnkSta: velocidade de 8 GT/s, largura x16

5 Instalação, upgrade e licenças do DDOS

5.1 DD6900/DD9400/DD9900

- Não é necessário ter licença
- Por padrão, instalado/ativado para todas as séries DD mais recentes (DD6900/DD9400/DD9900)

5.2 Equipamentos da geração anterior com a versão mais recente do DDOS

- Nenhum dispositivo de assistência de hardware disponível/compatível
- Nenhum impacto no processo de upgrade do DDOS
- O DDOS detecta automaticamente o número do modelo da plataforma

A Recursose suporte técnico

O foco do site Dell.com/support é atender às necessidades dos clientes com serviços e suporte comprovados.

A.1 Recursos relacionados

Equipamentos da série Dell EMC PowerProtect DD:

- Equipamentos da série Dell EMC PowerProtect DD
- Resumo da solução para equipamentos da série Dell EMC PowerProtect DD
- Planilha dos equipamentos da série Dell EMC PowerProtect DD
- Equipamentos da série Dell EMC PowerProtect DD com DDOS 7.5
- Equipamentos da série Dell EMC PowerProtect DD, a última geração de Data Domain Blog
- Folha de especificações dos equipamentos da série Dell EMC PowerProtect DD

Dell EMC PowerProtect DDOS

- Guia de administração do Dell EMC DDOS

Dell EMC DD OS

Version 7.0

Administration Guide

Revision 02
March 2020

DELL EMC

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

Preface

As part of an effort to improve its product lines, Dell EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features, software updates, software compatibility guides, and information about this product, licensing, and service.

Contact your technical support professional if a product does not function properly or does not function as described in this document.

Note: This document was accurate at publication time. Go to Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Purpose

This guide explains how to manage the PowerProtect DD Series Appliance systems with an emphasis on procedures using the dd System Manager, a browser-based graphical user interface (GUI). If an important administrative task is not supported in DD System Manager, the Command Line Interface (CLI) commands are described.

Note:

- DD System Manager was formerly known as the Enterprise Manager.
- In some cases, a CLI command may offer more options than those offered by the corresponding DD System Manager feature. See the *PowerProtect DD Series Appliances Operating System Command Reference Guide* for a complete description of a command and its options.

Audience

This guide is for system administrators who are familiar with standard backup software packages and general backup administration.

Related documentation

Additional DD OS documentation is available from: https://www.dell.com/support/article/us/en/04/sln318579/powerprotect-and-data-domain-core-documents

Special notice conventions used in this document

This document uses the following conventions for special notices:

NOTICE A notice identifies content that warns of a potential business or data loss.

Note: A note identifies information that is incidental, but not essential, to the topic. Notes can provide an explanation, a comment, reinforcement of a point in the text, or just a related point.

Typographical conventions

This document uses the following type style conventions in this document:

Table 1 Typography

Bold	Indicates interface element names, such as names of windows, dialog boxes, buttons, fields, tab names, key names, and menu paths (what the user specifically selects or clicks)

Table 1 Typography (continued)

Italic	Highlights publication titles listed in text
Monospace	Indicates system information, such as: • System code • System output, such as an error message or script • Pathnames, filenames, prompts, and syntax • Commands and options
Monospace italic	Highlights a variable name that must be replaced with a variable value
Monospace bold	Indicates text for user input
[ ]	Square brackets enclose optional values
|	Vertical bar indicates alternate selections—the bar means "or"
{ }	Braces enclose content that the user must specify, such as x or y or z
...	Ellipses indicate nonessential information omitted from the example

Where to get help

You can get support, product, and licensing information as follows:

Product information

For documentation, release notes, software updates, or information about this product, go to Online Support at https://support.emc.com.

Technical support

Go to Online Support and click Service Center. You will see several options for contacting Technical Support. Note that to open a service request, you must have a valid support agreement. Contact your sales representative for details about obtaining a valid support agreement or with questions about your account.

Your comments

Your suggestions will help us continue to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to: DPAD.Doc.Feedback@emc.com.

CHAPTER 1

System Features and Integration

This chapter includes:

Revision history

The revision history lists the major changes to this document to support DD OS Release 7.0.

Table 2 Document revision history

Revision	Date	Description
02 (7.0.0)	March 2020	This revision includes the following corrections and clarifications: • Corrected DD6900 and DD9400 MTree limits. • CAC/PIV card login • Removed an unsupported US location for configuring a cloud unit for Google. • Add the CLI steps to register the system with an ESRS gateway. • Added additional information about snapshot retention after breaking an MTree replication context. • Added additional information about licensing requirements for storage migration.
01 (7.0.0)	September 2019	This revision includes information about these new features: • Retention Lock Compliance for DD6900, DD9400, and DD9900 systems. • GUI support for system coredump management.

System overview

Data Domain and PowerProtect systems are disk-based inline deduplication appliances that provide data protection and disaster recovery (DR) in the enterprise environment.

Note: In this guide, "the protection system" or simply "the system" refers to both Data Domain and PowerProtect DD systems running DD OS 7.0 or later.

All protection systems run the DD OS, which provides both a command-line interface (CLI) for performing all system operations, and the DD System Manager graphical user interface (GUI) for configuration, management, and monitoring.

Note: DD System Manager was formerly known as the Enterprise Manager.

Protection systems consist of appliances that vary in storage capacity and data throughput. Systems are typically configured with expansion enclosures that add storage space.

System features

System features ensure data integrity, reliable restoration, efficient resource usage, and ease of management. Licensed features enable you to scale the system feature set to match your needs and budget.

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.
- An append-only write policy guards against overwriting valid data.
- 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 verify 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). Additionally, most configurations include a hot spare in each enclosure. Each parity stripe uses block checksums to ensure that data is correct. Checksums are constantly used during the online verify 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 non-volatile RAM (NVRAM) to track outstanding I/O operations. The following system models write the contesnts of the NVRAM to flash memory upon power failure or reboot to preserve that data indefinitely:
  - DD6300
  - DD6800
  - DD6900
  - DD9300
  - DD9400
  - DD9500
  - DD9800
  - DD9900
- When reading data back on a restore operation, the DD OS uses multiple layers of consistency checks to verify that restored data is correct.
- When writing to SSD cache, the DD OS:
  - Creates an SL checksum for every record stored in the cache to detect corruption to cache data. This checksum is validated for every cache read.
  - Treats corruption to cache data as a cache miss to avoid data loss by forcing clients to retrieve the most recent copy of the data from a different backup mechanism such as NVRAM or HDD instead of retrieving the corrupted data from the cache.

- Removes the need for inline verification of cache writes because end-to-end verification is performed on the copy of the data that resides on the system HDDs. This also saves I/O bandwidth by eliminating the need to perform additional I/O operations on the SSDs.
- Removes the need for continuous fault detection on the SSDs because the SSDs have a built-in scan capability.

Data deduplication

The file system deduplicates data by identifying redundant data during each backup and storing unique data just once.

The storage of unique data is invisible to backup software and independent of data format. Data can be structured, such as databases, or unstructured, such as text files. Data can derive from file systems or from raw volumes.

Typical deduplication ratios are 20-to-1, on average, over many weeks. This ratio assumes there are weekly full backups and daily incremental backups. A backup that includes many duplicate or similar files (files copied several times with minor changes) benefits the most from deduplication.

Depending on backup volume, size, retention period, and rate of change, the amount of deduplication can vary. The best deduplication happens with backup volume sizes of at least 10 MiB (MiB is the base 2 equivalent of MB).

To take full advantage of multiple systems, a site with more than one system must consistently backup the same client system or set of data to the same target system. For example, if a full back up of all sales data goes to target system A, maximum deduplication is achieved when the incremental backups and future full backups for sales data also go to target system A.

Restore operations

File restore operations create little or no contention with backup or other restore operations.

Incremental backups to the system are superior to tape backups, because they are always reliable and can be easily accessed.

You can perform full backups more frequently without the penalty of storing redundant data. Multiple processes can access the system simultaneously. The system enables your site to offer safe, user-driven, single-file restore operations.

DD Replicator

DD Replicator sets up and manages the replication of backup data between two protection systems.

A DD Replicator pair consists of a source and a destination system and replicates a complete data set or directory from the source system to the destination system. An individual system can be a part of multiple replication pairs and can serve as a source for one or more pairs and a destination for one or more pairs. After replication is started, the source system automatically sends any new backup data to the destination system.

Multipath and load balancing

In a Fibre Channel multipath configuration, multiple paths are established between a protection system and a backup server or backup destination array. When multiple paths are present, the system automatically balances the backup load between the available paths.

At least two HBA ports are required to create a multipath configuration. When connected to a backup server, each of the HBA ports on the multipath is connected to a separate port on the backup server.

High Availability

The High Availability (HA) feature lets you configure two protection systems as an Active-Standby pair, providing redundancy in the event of a system failure. HA keeps the active and standby systems in sync, so that if the active node were to fail due to hardware or software issues, the standby node can take over services and continue where the failing node left off.

The HA feature:

- Supports failover of backup, restore, replication and management services in a two-node system. Automatic failover requires no user intervention.
- Provides a fully redundant design with no single point of failure within the system when configured as recommended.
- Provides an Active-Standby system with no loss of performance on failover.
- Provides failover within 10 minutes for most operations. CIFS, DD VTL, and NDMP must be restarted manually.

  Note: Recovery of DD Boost applications may take longer than 10 minutes, because Boost application recovery cannot begin until the DD server failover is complete. In addition, Boost application recovery cannot start until the application invokes the Boost library. Similarly, NFS may require additional time to recover.
- Supports ease of management and configuration through DD OS CLI commands.
- Provides alerts for malfunctioning hardware.
- Preserves single-node performance and scalability within an HA configuration.

  Note: The active node continues retains full functionality, performance, and scalability even if the HA configuration is in degraded mode, which means the standby node is unavailable for failover.
- Supports the same feature set as stand-alone DD systems, with the exception of vDisk.
- Supports systems with all SAS drives. This includes legacy systems upgraded to systems with all SAS drives.

  Note: The Hardware Overview and Installation Guides for the systems that support HA describes how to install a new HA system. The *Single Node to HA Upgrade* describes how to upgrade an existing system to an HA pair.
- Does not impact the ability to scale the product.
- Supports nondisruptive software updates.

HA is supported on the following systems:

- Data Domain DD6800
- Power Protect DD6900
- Data Domain DD9300
- Power Protect DD9400
- Data Domain DD9500
- Data Domain DD9800
- Power Protect DD9900

HA architecture

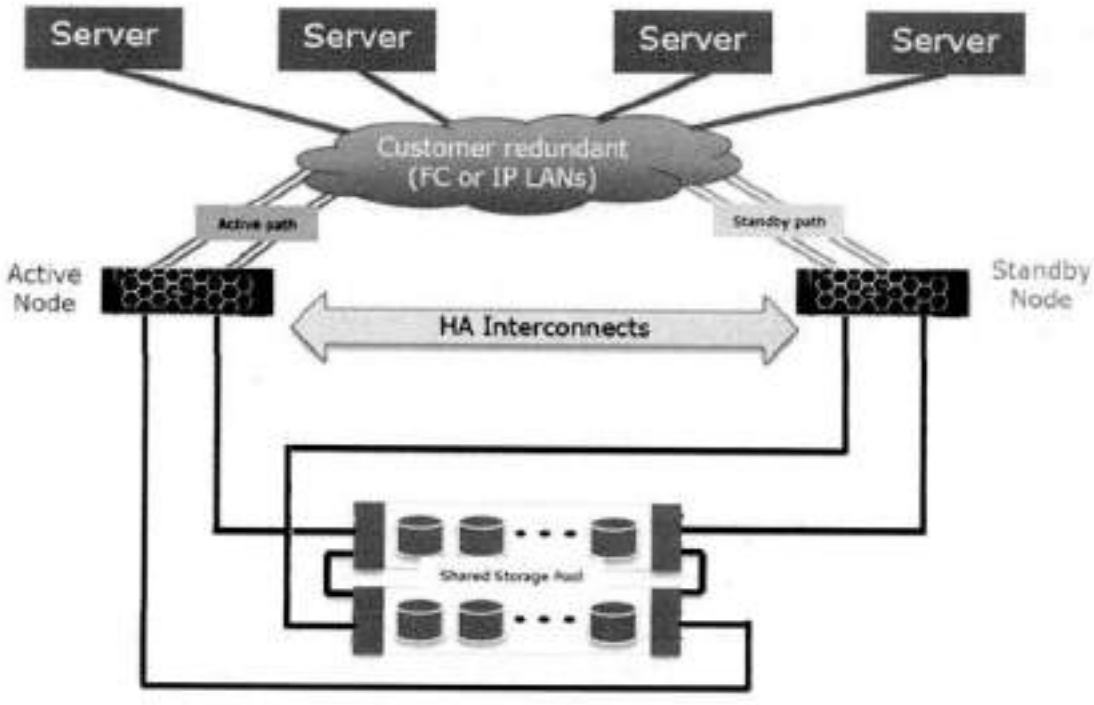
HA functionality is available for both IP and FC connections. Both nodes must have access to the same IP networks, FC SANs, and hosts in order to achieve high availability for the environment.

Over IP networks, HA uses a floating IP address to provide data access to the active node of the HA pair, regardless of which physical node is the active node.

Over FC SANs, HA uses NPIV to move the FC WWNs between nodes, allowing the FC initiators to re-establish connections after a failover.

Figure 1 on page 22 shows the HA architecture.

Figure 1 HA architecture



Random I/O handling

The random I/O optimizations included in DD OS provide improved performance for applications and use cases that generate larger amounts of random read and write operations than sequential read and write operations.

DD OS is optimized to handle workloads that consist of random read and write operations, such as virtual machine instant access and instant restore, and incremental forever backups generated by applications such as Avamar. These optimizations:

- Improve random read and random write latencies.
- Improve user IOPS with smaller read sizes.
- Support concurrent I/O operations within a single stream.
- Provide peak read and write throughput with smaller streams.

  Note: The maximum random I/O stream count is limited to the maximum restore stream count of a protection system.

The random I/O enhancements allow the protection system to support instant access/instant restore functionality for backup applications such as Avamar and Networker.

System administrator access

System administrators can access the system for configuration and management using a command line interface (CLI) or a graphical user interface (GUI).

- DD OS CLI - A command-line interface that is available through a serial console or through Ethernet connections using SSH or Telnet. CLI commands enable initial system configuration, changes to individual system settings, and display of system operation status.
- DD System Manager - A browser-based graphical user interface that is available through Ethernet connections. Use DD System Manager to perform initial system configuration, modify the system configuration, display system and component status, and generate reports and charts.

Note: Some DD hardware models support access using a keyboard and monitor attached directly to the system.

Licensed features

Feature licenses allow you to purchase only those features you intend to use. Some examples of features that require licenses are DD Boost, and capacity on demand (storage capacity increases).

Consult with your sales representative for information on purchasing licensed features.

Table 3 Features requiring licenses

Feature Name	License Name in Software	Description
DD ArchiveStore	ARCHIVESTORE	Licenses systems for archive use, such as file and email archiving, file tiering, and content and database archiving.
DD Boost	DDBOOST	Enables the use of a system with qualified backup software. The online compatibility guide available at https://compatibilityguide.emc.com:8080/CompGuideApp/ provides the list of qualified applications. The managed file replication (MFR) feature of DD Boost also requires the DD Replicator license.
DD Capacity on Demand	CONTROLLER-COD	Enables an on-demand capacity increase for a DD system that is not at its maximum supported capacity.
Cloud Tier	CLOUDTIER-CAPACITY	Enables a system to move data from the active tier to low-cost, high-capacity object storage in the public, private, or hybrid cloud for long-term retention.
DD Encryption	ENCRYPTION	Allows data on system drives or external storage to be encrypted while being saved and locked when moving the system to another location.
DD Expansion Storage	EXPANDED-STORAGE	Allows system storage to be expanded beyond the level provided in the base system.

Table 3 Features requiring licenses (continued)

Feature Name	License Name in Software	Description
DD I/OS (for IBM i operating environments)	I/OS	An I/OS license is required when DD VTL is used to backup systems in the IBM i operating environment. Apply this license before adding virtual tape drives to libraries.
DD Replicator	REPLICATION	Adds DD Replicator for replication of data from one protection system to another. A license is required on each system.
DD Retention Lock Compliance Edition	RETENTION-LOCK-COMPLIANCE	Meets the strictest data retention requirements from regulatory standards such as SEC17a-4.
DD Retention Lock Governance Edition	RETENTION-LOCK-GOVERNANCE	Protects selected files from modification and deletion before a specified retention period expires.
DD Shelf Capacity-Active Tier	CAPACITY-ACTIVE	Enables a system to expand the active tier storage capacity to an additional enclosure or a disk pack within an enclosure.
DD Storage Migration	STORAGE-MIGRATION-FOR-DATADOMAIN-SYSTEMS	Enables migration of data from one enclosure to another to support replacement of older, lower-capacity enclosures.
DD Virtual Tape Library (DD VTL)	VTL	Enables the use of a protection system as a virtual tape library over a Fibre Channel network. This license also enables the NDMP Tape Server feature, which previously required a separate license.
High Availability	HA-ACTIVE-PASSIVE	Enables the High Availability feature in an Active-Standby configuration. You only need to purchase one HA license; the license runs on the active node and is mirrored to the standby node.
SSD Cache	SSD-CAPACITY	Enables the SSD cache feature on DD6300, DD6800, DD9300, DD9500, and DD9800 systems. This license is not required to use the SSD cache feature on DD6900, DD9400, and DD9900 systems.

Storage environment integration

Protection systems integrate easily into existing data centers.

- All protection systems can be configured as storage destinations for leading backup and archiving applications using NFS, CIFS, DD Boost, or DD VTL protocols.
- Search for *compatibility documents* at https://support.emc.com for information on the applications that work with the different configurations.
- Multiple backup servers can share a single protection system.

- A single protection system can handle multiple simultaneous backup and restore operations.
- Multiple protection systems can be connected to one or more backup servers.

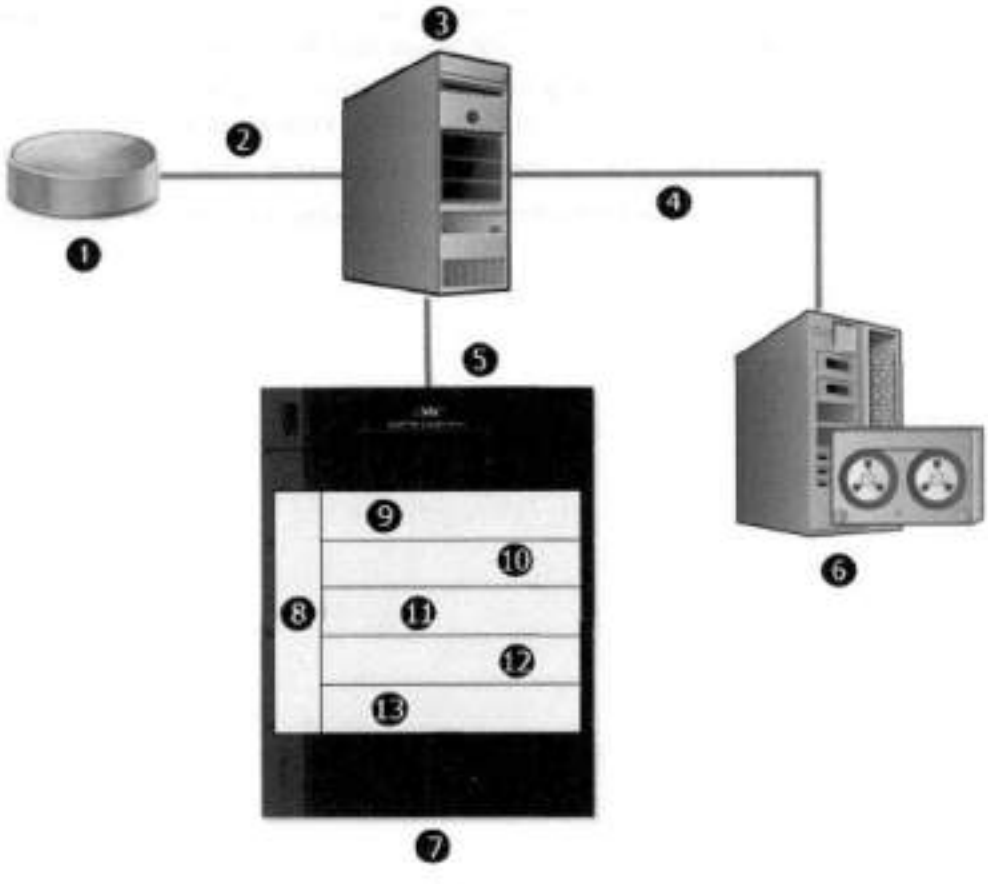
For use as a backup destination, a protection system can be configured either as a disk storage unit with a file system that is accessed through an Ethernet connection or as a virtual tape library that is accessed through a Fibre Channel connection. The DD VTL feature enables protection systems to be integrated into environments where backup software is already configured for tape backups to minimize disruption.

Configuration is performed both in the DD OS, as described in the relevant sections of this guide, and in the backup application, as described in the backup application's administrator guides and in application-related guides and tech notes.

All backup applications can access the protection system as either an NFS or a CIFS file system on the disk device.

The following figure shows a protection system integrated into an existing basic backup configuration.

Figure 2 Protection system integrated into a storage environment



1. Primary storage
2. Ethernet
3. Backup server
4. SCSI/Fibre Channel
5. Ethernet or Fibre Channel connection
6. Tape system

Figure 2 Protection system integrated into a storage environment (continued)

7. Protection system
8. DD OS management layer
9. NFS export/CIFS share/DD VTL pool/DD Boost storage unit
10. DD OS data verification
11. DD OS file system
12. DD OS global deduplication and compression
13. DD OS RAID protection

As shown in Figure 2 on page 25, data flows to the protection system through an Ethernet or Fibre Channel connection. Immediately, the data verification processes begin and are continued while the data resides on the system. In the file system, the DD OS Global Compression algorithms deduplicate and compress the data for storage. Data is then sent to the disk RAID subsystem. When a restore operation is required, data is retrieved from storage, decompressed, verified for consistency, and transferred via Ethernet to the backup servers using Ethernet (for NFS, CIFS, DD Boost), or using Fiber Channel (for DD VTL and DD Boost).

The DD OS accommodates relatively large streams of sequential data from backup software and is optimized for high throughput, continuous data verification, and high compression. It also accommodates the large numbers of smaller files in nearline storage (DD ArchiveStore).

Protection system performance is best when storing data from applications that are not specifically backup software under the following circumstances.

- Data is sent to the protection system as sequential writes (no overwrites).
- Data is neither compressed nor encrypted before being sent to the protection system.

CHAPTER 2

Getting Started

This chapter includes:

Dell EMC DD System Manager overview

DD System Manager is a browser-based GUI for managing a single system from any location. DD System Manager provides a single, consolidated management interface that enables you to configure and monitor many of the system features and settings.

Note: PowerProtect DD Management Center (DDMC) enables you to manage multiple systems from a single browser window.

DD System Manager provides real-time graphs and tables that enable you to monitor the status of system hardware components and configured features.

Additionally, a command set that performs all system functions is available to users through the CLI. Commands configure system settings and display system hardware status, feature configuration, and operation.

The command-line interface is available through a serial console or through an Ethernet connection using SSH, Telnet, or serial over LAN (SOL).

Note: Some systems support access using a keyboard and monitor attached directly to the system.

DD OS Software Versions

DD OS software releases have two public statuses, indicating the number of installed systems running the version.

- **General Availability** releases have completed internal QA Testing and are available for installation in production environments.
- **Directed Availability - Controlled (Directed Availability)** releases are carefully controlled access releases, directed to a small number of installations. Customers may request to be qualified for access to these releases.
- **Target Code** -Dell EMC recommends that all systems upgrade to the DD OS target code within a release family as soon as practical.

  Note: There is only one Target Code release in a given family. Target Code releases have met the installation and run-time hours and quality metrics to indicate that they are stable and have no problems that would affect most customers. For some release families, there may be no target code identified, due to limited customer uptake, quality issues, or other considerations.

Upgrading between families may have product compatibility considerations, and a careful review of product compatibility should precede any upgrade to a new release family.

Logging in and out of DD System Manager

DD System Manager provides a single, consolidated management interface that enables you to configure and monitor many of the system features and settings Use a browser to log in to DD System Manager.

About this task

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

Note: For information about managing user permissions, see the KB article *Managing User Permissions on the Data Domain system*, available from the Online Support website, at https://support.emc.com/kb/181533.

Procedure

1. Open a web browser and enter the IP address or hostname to connect to DD System Manager. It must be one of the following:
   - A fully qualified domain name (for example, `http://dd01.example.com`)
   - A hostname (`http://dd01`)
   - An IP address (`http://10.5.50.5`)

   Note: DD System Manager uses HTTP port 80 and HTTPS port 443. If your system is behind a firewall, you may need to enable port 80 if using HTTP, or port 443 if using HTTPS to reach the system. The port numbers can be easily changed if security requirements dictate.

   Note: If DD System Manager is unable to launch from any web browser, the displayed error message is "The GUI Service is temporarily unavailable. Please refresh your browser. If the problem persists, contact support for assistance." SSH can be used to login to the system and can run all commands.
   If you have not upgraded the DD OS but still encounter this GUI error, use the following procedure:

   a. Close the web browser session on the system with the reported error.

   b. Run these commands in sequence:
      - `adminaccess disable http`
      - `adminaccess disable https`
      - `adminaccess enable http`
      - `adminaccess enable https`

   c. Wait 5 minutes to allow the http and https services to start completely.

   d. Open a web browser, and connect to DD System Manager.

   If you see this GUI issue after a DD OS upgrade, use the following procedure:

   a. Close the web browser session on the system with the reported error.

   b. Run these commands in sequence:
      - `adminaccess disable http`
      - `adminaccess disable https`
      - `adminaccess certificate generate self-signed-cert`
      - `adminaccess enable http`
      - `adminaccess enable https`

   a. Wait 5 minutes to allow the http and https services to start completely.

   b. Open a web browser, and connect to DD System Manager.

2. For HTTPS secure login, click **Secure Login**.

   Secure login with HTTPS requires a digital certificate to validate the identity of the DD OS system and to support bi-directional encryption between DD System Manager and a browser. DD OS includes a self-signed certificate, and DD OS allows you to import your own certificate.

3. Enter your assigned username and password.

- For physical systems the default password is the system serial number.
- For PowerProtect DD Virtual Edition (DD VE) instances the default password is `changeme`.

4. Click **Log In**.

   If this is the first time you have logged in, the Home view is displayed in the Information panel.

   Note: If you enter an incorrect password 4 consecutive times, the system locks out the specified username for 120 seconds. The login count and lockout period are configurable and might be different on your system.

   Note: If this is the first time you are logging in, you might be required to change your password. If the system administrator has configured your username to require a password change, you must change the password before gaining access to DD System Manager.

   If you forget the sysadmin password after changing it, contact Dell EMC Support.

5. To log out, click the log out button in the DD System Manager banner.

   When you log out, the system displays the log in page with a message that your log out is complete.

Log in with certificate using CAC/PIV card

Log in to DD System Manager with a certificate issued by a Certificate Authority (CA).

Before you begin

- You must have authorization privileges on the protection system, and the protection system must trust the CA certificate. Your username must be specified in the common-name field in the certificate.
- You must have a user account on the protection system. You can be either a local user or a name service user (NIS/AD). For a name service user, your group-to-role mapping must be configured on the protection system.

Procedure

1. Use the following CLI command to import the public key from the CA that issued the certificate: `adminaccess certificate import ca application login-auth`.
2. Load the user certificate in PKCS12 format in your browser from the CAC/PIV card after swiping CAC/PIV card against a card reader which interacts with the browser .

   Once the CA certificate is trusted by the protection system, a **Log in with certificate** link is visible on the HTTPS login screen.

3. Click **Log in with certificate**, and choose the user certificate from the list of certificates that are prompted by the browser.

Results

The system validates the user certificate against the trust store. Based on authorization privileges associated with your account, a System Manager session is created for you.

Logging in using single sign-on (SSO)

As an alternative to logging in using a local username and password, you can log in to DD System Manager with a username and password from a supported SSO provider .

Before you begin

To log in using SSO, SSO must be enabled and the protection system must be registered with an SSO provider.

About this task

Configuring SSO authentication on page 155 describes how to enable SSO authentication and register the protection system with the SSO provider.

Procedure

1. At the login screen, click **Log in with Data Protection Central**.

   Note: If a brand name is set on Data Protection Central (DPC), the link appears as **Log in with** ***<DPC-brand-name>***.

2. Log in with the DPC username and password.

The DD System Manager interface

The DD System Manager interface provides common elements on most pages that enable you to navigate through the configuration and display options, and context sensitive help.

Page elements

The primary page elements are the banner, the navigation panel, the information panels, and footer.

Figure 3 DD System Manager page components

1. Banner
2. Navigation panel
3. Information panels
4. Footer

Banner

The DD System Manager banner displays the program name and buttons for **Refresh**, **Log Out**, and **Help**.

Navigation panel

The Navigation panel displays the highest level menu selections that you can use to identify the system component or task that you want to manage.

The Navigation panel displays the top two levels of the navigation system. Click any top level title to display the second level titles. Tabs and menus in the Information panel provide additional navigation controls.

Information panel

The Information panel displays information and controls related to the selected item in the Navigation panel, and is where you find system status information and configure a system.

Depending on the feature or task selected in the Navigation panel, the Information panel may display a tab bar, topic areas, table view controls, and the More Tasks menu.

Tab bar

Tabs provide access to different aspects of the topic selected in the Navigation panel.

Topic areas

Topic areas divide the Information panel into sections that represent different aspects of the topic selected in the Navigation panel or parent tab.

For high-availability (HA) systems, the HA Readiness tab on the System Manager dashboard indicates whether the HA system is ready to fail over from the active node to the standby node. You can click on **HA Readiness** to navigate to the **High Availability** section under **HEALTH**.

Working with table view options

Many of the views with tables of items contain controls for filtering, navigating, and sorting the information in the table.

How to use common table controls:

- Click the diamond icon in a column heading to reverse the sort order of items in the column.
- Click the < and > arrows at the bottom right of the view to move forward or backward through the pages. To skip to the beginning of a sequence of pages, click **|<**. To skip to the end, click **>|**.
- Use the scroll bar to view all items in a table.
- Enter text in the **Filter By** box to search for or prioritize the listing of those items.
- Click **Update** to refresh the list.
- Click **Reset** to return to the default listing.

More Tasks menu

Some pages provide a More Tasks menu at the top right of the view that contains commands related to the current view.

Footer

The DD System Manager footer displays important information about the management session.

The footer lists the following information.

- System hostname.
- DD OS version
- Selected system model number.
- User name and role for the current logged in user.

Help buttons

Help buttons display a ? and appear in the banner, in the title of many areas of the Information panel, and in many dialog boxes. Click the help button to display a help window related to the current feature you are using.

The help window provides a contents button and navigation button above the help. Click the contents button to display the guide contents and a search button that you can use to search the help. Use the directional arrow buttons to page through the help topics in sequential order.

End User License Agreement

To view the End User License Agreement (EULA), select **Maintenance** > **System** > **View EULA**.

Configuring the system with the configuration wizard

The protection system provides two wizards: a DD System Manager configuration wizard and a Command Line Interface (CLI) configuration wizard. The configuration wizards guide you through a simplified configuration of your system to get your protection system operating quickly.

About this task

After you complete the basic configuration with a wizard, you can use additional configuration controls in DD System Manager and the CLI to further configure your system.

Note: The following procedure describes how to start and run the DD System Manager configuration wizard after the initial configuration of your protection system. For instructions on running the configuration wizards at system startup, see the *Installation Guide* for your system model.

Note: To configure your system for HA, use the CLI Configuration Wizard. For more information, see the *Installation Guide* for the HA-capable system.

Procedure

1. Select **Maintenance** > **System** > **Configure System**.
2. Use the controls at the bottom of the Configuration Wizard dialog box to select which features to configure and to advance through the wizard. To display help for a feature, click the help icon (question mark) in the lower left corner of the dialog box.

License page

The License page displays all installed licenses. Click **Yes** to add, modify, or delete a license, or click **No** to skip license installation.

License Configuration

The **Licenses Configuration** section enables you add, modify, or delete licenses from a license file. DD OS 6.0 and later supports licensing via the Electronic License Management System (ELMS), which enables you to include multiple features in a single license file upload.

When using the Configuration Wizard on a system with no licenses configured, select the license type from the drop-down, and click the ... button. Browse to the directory where the license file resides, and select it for upload to the system.

Table 4 License Configuration page values

Item	Description
Add Licenses	Select this option to add licenses from a license file.
Replace Licenses	If licenses are already configured the **Add Licenses** selection changes to **Replace Licenses**. Select this option to replace the licenses already added.
Delete Licenses	Select this option to delete licenses already configured on the system.

Network

The **Network** section enables you to configure the network settings. Click **Yes** to configure the network settings, or click **No** to skip network configuration.

Network General page

The General page enables you to configure network settings that define how the system participates in an IP network.

To configure these network settings outside of the configuration wizard, select **Hardware** > **Ethernet**.

Table 5 General page settings

Item	Description
Obtain Settings using DHCP	Select this option to specify that the system collect network settings from a Dynamic Host Control Protocol (DHCP) server. When you configure the network interfaces, at least one of the interfaces should be configured to use DHCP.
Manually Configure	Select this option to use the network settings defined in the Settings area of this page.
Host Name	Specifies the network hostname for this system. ⓘ Note: If you choose to obtain the network settings through DHCP, you can manually configure the hostname at **Hardware** > **Ethernet** > **Settings** or with the `net set hostname` command. You must manually configure the host name when using DHCP over IPv6.
Domain Name	Specifies the network domain to which this system belongs.
Default IPv4 Gateway	Specifies the IPv4 address of the static default gateway to which the system will forward network requests when there is no route entry for the destination system.
Default IPv6 Gateway	Specifies the IPv6 address of the static default gateway to which the system will forward network requests when there is no route entry for the destination system.

Network Interfaces page

The Interfaces page enables you to configure network settings that define how each interface participates in an IP network.

To Configure these network settings outside of the configuration wizard, select **Hardware** > **Ethernet** > **Interfaces**.

Table 6 Interfaces page settings

Item	Description
Interface	Lists the interfaces available on your system.
Enabled	Shows whether each interface is enabled (checkbox selected) or disabled (not selected). Click the checkbox to toggle the interface between the enabled and disabled states.

Table 6 Interfaces page settings (continued)

Item	Description
DHCP	Shows the current Dynamic Host Control Protocol (DHCP) configuration for each interface. Select **v4** for IPv4 DHCP connections, **v6** for IPv6 connections, or **no** to disable DHCP.
IP Address	Specifies an IPv4 or IPv6 address for an interface on this system. To configure the IP address, you must set DHCP to **No**.
Netmask	Specifies the network mask for this system. To configure the network mask, you must configure a static IP address and set DHCP to **No**.
Link	Displays whether the Ethernet link is active (Yes) or not (No).

Network DNS page

The DNS page enables you to configure IP addresses for DNS servers to convert hostnames to IP addresses and vice versa.

To Configure these network settings outside of the configuration wizard, select **Hardware** > **Ethernet** > **Settings**.

Table 7 DNS page settings

Item	Description
Obtain DNS using DHCP.	Select this option to specify that the system collect DNS IP addresses from a Dynamic Host Control Protocol (DHCP) server. When you configure the network interfaces, at least one of the interfaces should be configured to use DHCP.
Manually configure DNS list.	Select this option when you want to manually enter DNS server IP addresses.
Add (+) button	Click this button to display a dialog box in which you can add a DNS IP address to the DNS IP Address list. You must select **Manually configure DNS list** before you can add or delete DNS IP addresses.
Delete (X) button	Click this button to delete a DNS IP address from the DNS IP Address list. You must select the IP address to delete before this button is enabled. You must also select **Manually configure DNS list** before you can add or delete DNS IP addresses.
IP Address Checkboxes	Select a checkbox for a DNS IP address that you want to delete. Select the DNS IP Address checkbox when you want to delete all IP addresses. You must select **Manually configure DNS list** before you can add or delete DNS IP addresses.

File System

The **File System** section allows you to create the file system, and configure Active Tier, Cache Tier, and Cloud Tier storage. Each has a separate wizard page. The configuration pages cannot be accessed if the file system is already created.

Cache Tier storage is part of the configuration wizard for the following system models that come with SSDs for cache storage:

- DD6900
- DD9400
- DD9900

Cloud Tier storage is optional, and you can configure it later. The file system must be disabled to configure Cloud Tier storage.

Anytime you display the **File System** section when the File System has not been created, the system displays an error message. Continue with the procedure to create the file system.

Configure storage tier pages

The configure storage tier pages enable you to configure storage for each licensed tier on the system, Active Tier, Cache Tier, and Cloud Tier. Each tier has a separate wizard page. The storage tier configuration pages cannot be accessed through the wizard if the file system is already created.

Systems that use 8 TB disks require a certain number of disks installed in the disk shelves in order to configure Active Tier and Cloud Tier storage. The minimum disk requirements are:

ⓘ Note: Systems that are not listed in this table do not support 8 TB disks, and are not subject to this requirement.

System	Minimum disk packs required for Active Tier (number of disks)	Minimum disk packs required for Cloud Tier (number of disks)
DD6900	N/A	2 packs (30 disks)
DD9400	4 packs (60 disks)	4 packs (60 disks)
DD9900	8 packs (120 disks)	5 packs (75 disks)

Configure Active Tier

The Configure Active Tier section allows you to configure the Active Storage Tier devices. The Active Tier is where back up data resides. To add storage to the Active Tier, select one or more devices and add them to the tier. You can add storage devices up to the capacity licenses installed.

ⓘ Note: The DD3300 system requires 4 TB devices for the Active Tier.

Table 8 Addable Storage

Item	Description
ID (Device in DDVE)	The disk identifier, which can be any of the following. • The enclosure and disk number (in the form Enclosure Slot, or Enclosure Pack for DS60 shelves) • A device number for a logical device such as those used by DD VTL and vDisk

Table 8 Addable Storage (continued)

Item	Description
	• A LUN
Disks	The disks that comprise the disk pack or LUN. This does not apply to DDVE instances.
Model	The type of disk shelf. This does not apply to DDVE instances.
Disk Count	The number of disks in the disk pack or LUN. This does not apply to DDVE instances.
Disk Size (Size in DDVE)	The data storage capacity of the disk.[a]
Failed Disks	Failed disks in the disk pack or LUN. This does not apply to DDVE instances.
Type	SCSI. This only applies to DDVE instances.

a. The DD OS convention for computing disk space defines one gibibyte as 2^{30} bytes, giving a different disk capacity than the manufacturer's rating.

Table 9 Active Tier values

Item	Description
ID (Device in DDVE)	The disk identifier, which can be any of the following. • The enclosure and disk number (in the form Enclosure Slot, or Enclosure Pack for DS60 shelves). This does not apply to DDVE instances. • A device number for a logical device such as those used by DD VTL and vDisk • A LUN
Disks	The disks that comprise the disk pack or LUN. This does not apply to DDVE instances.
Model	The type of disk shelf. This does not apply to DDVE instances.
Disk Count	The number of disks in the disk pack or LUN. This does not apply to DDVE instances.
Disk Size (Size in DDVE)	The data storage capacity of the disk.[a]
Failed Disks	Failed disks in the disk pack or LUN. This does not apply to DDVE instances.
Configured	New or existing storage. This does not apply to DDVE instances.
Type	SCSI. This only applies to DDVE instances.

a. The DD OS convention for computing disk space defines one gibibyte as 2^{30} bytes, giving a different disk capacity than the manufacturer's rating.

Configure Cache Tier

The Configure Cache Tier section allows you to configure the Cache Storage Tier devices. The Cache Tier is where metadata cached with the Metadata on Flash feature resides. To add storage

to the Cache Tier, select one or more devices and add them to the tier. You can add storage devices up to the capacity licenses installed.

Note: DD6900, DD9400, and DD9900 systems do not require a license for Cache Tier storage.

Table 10 Addable Storage

Item	Description
ID	The disk identifier, which can be any of the following. • The enclosure and disk number (in the form Enclosure Slot, or Enclosure Pack for DS60 shelves) • A device number for a logical device such as those used by DD VTL and vDisk • A LUN
Disk Size (Size in DDVE)	The data storage capacity of the disk.[a]
Type	SAS-SSD

a. The DD OS convention for computing disk space defines one gibibyte as 2^{30} bytes, giving a different disk capacity than the manufacturer's rating.

Table 11 Cache Tier values

Item	Description
ID	The disk identifier, which can be any of the following. • The enclosure and disk number (in the form Enclosure Slot, or Enclosure Pack for DS60 shelves). This does not apply to DDVE instances. • A device number for a logical device such as those used by DD VTL and vDisk • A LUN
Disk Size (Size in DDVE)	The data storage capacity of the disk.[a]
Type	SAS-SSD
Configured	New or existing storage.

a. The DD OS convention for computing disk space defines one gibibyte as 2^{30} bytes, giving a different disk capacity than the manufacturer's rating.

Configure Cloud Tier

The Configure Cloud Tier section allows you to configure the Cloud Storage Tier devices. To add storage to the Cloud Tier, select one or more devices and add them to the tier. You can add storage devices up to the capacity licenses installed.

Note: The DD3300 system requires 1 TB devices for Cloud Tier.

Table 12 Addable Storage

Item	Description
ID (Device in DDVE)	The disk identifier, which can be any of the following.

Table 12 Addable Storage (continued)

Item	Description
	• The enclosure and disk number (in the form Enclosure Slot, or Enclosure Pack for DS60 shelves) • A device number for a logical device such as those used by DD VTL and vDisk • A LUN
Disks	The disks that comprise the disk pack or LUN. This does not apply to DDVE instances.
Model	The type of disk shelf. This does not apply to DDVE instances.
Disk Count	The number of disks in the disk pack or LUN. This does not apply to DDVE instances.
Disk Size (Size in DDVE)	The data storage capacity of the disk.[a]
License Needed	The licensed capacity required to add the storage to the tier.
Failed Disks	Failed disks in the disk pack or LUN. This does not apply to DDVE instances.
Type	SCSI. This only applies to DDVE instances.

a. The DD OS convention for computing disk space defines one gibibyte as 2^{30} bytes, giving a different disk capacity than the manufacturer's rating.

Table 13 Cloud Tier values

Item	Description
ID (Device in DDVE)	The disk identifier, which can be any of the following. • The enclosure and disk number (in the form Enclosure Slot, or Enclosure Pack for DS60 shelves). This does not apply to DDVE instances. • A device number for a logical device such as those used by DD VTL and vDisk • A LUN
Disks	The disks that comprise the disk pack or LUN. This does not apply to DDVE instances.
Model	The type of disk shelf. This does not apply to DDVE instances.
Disk Count	The number of disks in the disk pack or LUN. This does not apply to DDVE instances.
Disk Size (Size in DDVE)	The data storage capacity of the disk.[a]
License Used	The licensed capacity consumed by the storage.
Failed Disks	Failed disks in the disk pack or LUN. This does not apply to DDVE instances.
Configured	New or existing storage. This does not apply to DDVE instances.
Type	SCSI. This only applies to DDVE instances.

Table 13 Cloud Tier values (continued)

a. The DD OS convention for computing disk space defines one gibibyte as 2^{30} bytes, giving a different disk capacity than the manufacturer's rating.

Create File System page

The Create File System page displays the allowed size of each storage tier in the file system, and provides a setting to automatically enable the file system after it is created.

System Settings

The **System Settings** section enables you to configure system passwords and email settings. Click **Yes** to configure the system settings or click **No** to skip system settings configuration.

System Settings Administrator page

The Administrator page enables you to configure the administrator password and define how the system communicates with the administrator.

Table 14 Administrator page settings

Item	Description
User Name	The default administrator name is *sysadmin*. The sysadmin user cannot be renamed or deleted.
Old Password	Type the old password for sysadmin.
New Password	Type the new password for sysadmin.
Verify New Password	Retype the new password for sysadmin.
Admin Email	Specify the email address to which DD System Manager sends alert and autosupport email messages.
Send Alert Notification Emails to this address	Check to configure DD System Manager to send alert notifications to the Admin email address as alert events occur.
Send Daily Alert Summary Emails to this address	Check to configure DD System Manager to send alert summaries to the Admin email address at the end of each day.
Send Autosupport Emails to this address	Check to configure DD System Manager to send the Admin user autosupport emails, which are daily reports that document system activity and status.

System Settings Email/Location page

The Email/Location page enables you to configure the mail server name, control what system information is sent to Dell EMC, and specify a location name to identify your system.

Table 15 Email/Location page settings

Item	Description
Mail Server	Specify the name of the mail server that manages emails to and from the system.

Table 15 Email/Location page settings (continued)

Item	Description
Credentials	Select whether or not to require credentials for the mail server.
User Name	If credentials are enabled, specify the mail server username.
Password	If credentials are enabled, specify the mail server password.
Send Alert Notification Emails to Dell EMC	Check to configure DD System Manager to send alert notification emails to Dell EMC.
Send Vendor Support Notification Emails to Dell EMC	Check to configure DD System Manager to send vendor support notification emails to Dell EMC.
Location	Use this optional attribute to record the location of your system. If you specify a location, this information is stored as the SNMP system location.

DD Boost protocol

The **DD Boost** settings section enables you to configure the DD Boost protocol settings. Click **Yes** to configure the DD Boost Protocol settings, or click **No** to skip DD Boost configuration.

DD Boost Protocol Storage Unit page

The Storage Unit page enables you to configure DD Boost storage units.

To configure these settings outside of the configuration wizard, select **Protocols** > **DD Boost** > **Storage Units** > **+ (plus sign)** to add a storage unit, **the pencil** to modify a storage unit, or **X** to delete a storage unit.

Table 16 Storage Unit page settings

Item	Description
Storage Unit	The name of your DD Boost Storage Unit. You may optionally change this name.
User	For the default DD Boost user, either select an existing user, or select Create a new Local User, and enter their User name, Password, and Management Role. This role can be one of the following: • *Admin role*: Lets you configure and monitor the entire protection system. • *User role*: Lets you monitor systems and change your own password. • *Security role*: In addition to user role privileges, lets you set up security-officer configurations and manage other security-officer operators. • *Backup-operator role*: In addition to user role privileges, lets you create snapshots, import and export tapes to, or move tapes within a DD VTL.

Table 16 Storage Unit page settings (continued)

Item	Description
	• *None role*: Intended only for DD Boost authentication, so you cannot monitor or configure a system. None is also the parent role for the SMT tenant-admin and tenant-user roles. None is also the preferred user type for DD Boost storage owners. Creating a new local user here only allows that user to have the "none" role.

DD Boost Protocol Fibre Channel page

The Fibre Channel page enables you to configure DD Boost Access Groups over Fibre Channel.

To configure these settings outside of the configuration wizard, select **Protocols** > **DD Boost** > **Fibre Channel** > **+ (plus sign)** to add an access group, **the pencil** to modify an access group, or **X** to delete an access group.

Table 17 Fibre Channel page settings

Item	Description
Configure DD Boost over Fibre Channel	Select the checkbox if you want to configure DD Boost over Fibre Channel.
Group Name (1-128 Chars)	Create an Access Group. Enter a unique name. Duplicate access groups are not supported.
Initiators	Select one or more initiators. Optionally, replace the initiator name by entering a new one. An initiator is a backup client that connects to the system to read and write data using the FC (Fibre Channel) protocol. A specific initiator can support DD Boost over FC or DD VTL, but not both.
Devices	The devices to be used are listed. They are available on all endpoints. An endpoint is the logical target on the Data Domain or PowerProtect system to which the initiator connects.

CIFS protocol

The **CIFS Protocol** settings section enables you to configure the CIFS protocol settings. Click **Yes** to configure the CIFS protocol settings, or click **No** to skip CIFS configuration.

The system uses the term MTree to describe directories. When you configure a directory path, DD OS creates an MTree where the data will reside.

CIFS Protocol Authentication page

The Authentication page enables you to configure Active Directory and Workgroup for your system.

To configure these settings outside of the configuration wizard, select **Administration** > **Access** > **Authentication**.

Table 18 Authentication page settings

Item	Description
Active Directory/Kerberos Authentication	Expand this panel to enable, disable, and configure Active Directory Kerberos authentication.
Workgroup Authentication	Expand this panel to configure Workgroup authentication.
LDAP Authentication	Expand this panel to configure LDAP authentication.
NIS Authentication	Expand this panel to configure NIS authentication.

CIFS Protocol Share page

The Share page enables you to configure a CIFS protocol share name and a directory path for your system.

To configure these settings outside of the configuration wizard, select **Protocols** > **CIFS** > **Shares** > **Create**.

Table 19 Share page settings

Item	Description
Share Name	Enter a share name for the system.
Directory Path	Enter a directory path for the system.
Add (+) button	Click + to enter a system client, user, or group.
Pencil icon	Modify a client, user, or group.
Delete (X) button	Click X to delete a selected client, user, or group.

NFS protocol

The **NFS Protocol** settings section enables you to configure the NFS protocol settings. Click **Yes** to configure the NFS protocol settings, or click **No** to skip NFS configuration.

The system uses the term MTree to describe directories. When you configure a directory path, DD OS creates an MTree where the data will reside.

NFS Protocol Export page

The Export page enables you to configure an NFS protocol export directory path, network clients, and NFSv4 referrals.

To configure these settings outside of the configuration wizard, select **Protocols** > **NFS** > **Create**.

Table 20 Export page settings

Item	Description
Directory Path	Enter a pathname for the export.
Add (+) button	Click + to enter a system client or NFSv4 referral.
Pencil icon	Modify a client or NFSv4 referral.
Delete (X) button	Click X to delete a selected client or NFSv4 referral.

DD VTL protocol

The **DD VTL Protocol** settings section enables you to configure the DD Virtual Tape Library settings. Click **Yes** to configure the DD VTL settings, or click **No** to skip DD VTL configuration.

VTL Protocol Library page

The Library page enables you to configure the DD VTL protocol settings for a library.

To configure these settings outside of the configuration wizard, select **PROTOCOLS** > **VTL** > **Virtual Tape Libraries** > **VTL Service** > **Libraries** > **More Tasks** > **Library** > **Create**

Table 21 Library page settings

Item	Description
Library Name	Enter a name of from 1 to 32 alphanumeric characters.
Number of Drives	Number of supported tape drives.
Drive Model	Select the desired model from the drop-down list: • IBM-LTO-1 • IBM-LTO-2 • IBM-LTO-3 • IBM-LTO-4 • IBM-LTO-5 (default) • HP-LTO-3 • HP-LTO-4
Number of Slots	Enter the number of slots per library: • Up to 32,000 slots per library • Up to 64,000 slots per system • This should be equal to, or greater than, the number of drives.
Number of CAPs	(Optional) Enter the number of cartridge access ports (CAPs): • Up to 100 CAPs per library • Up to 1000 CAPs per system
Changer Model Name	Select the desired model from the drop-down list: • L180 (default) • RESTORER-L180 • TS3500 • I2000 • I6000 • DDVTL
Starting Barcode	Enter the desired barcode for the first tape, in the format A990000LA.

Table 21 Library page settings (continued)

Item	Description
Tape Capacity	(Optional) Enter the tape capacity. If not specified, the capacity is derived from the last character of the barcode.

VTL Protocol Access Group page

The Access Group page enables you to configure DD VTL protocol settings for an access group.

To configure these settings outside of the configuration wizard, select **PROTOCOLS** > **VTL** > **Access Groups** > **Groups** > **More Tasks** > **Group** > **Create**.

Table 22 Access Group page settings

Item	Description
Group Name	Enter a unique name of from 1 - 128 characters. Duplicate access groups are not supported.
Initiators	Select one or more initiators. Optionally, replace the initiator name by entering a new one. An initiator is a backup client that connects to a system to read and write data using the Fibre Channel (FC) protocol. A specific initiator can support DD Boost over FC or DD VTL, but not both.
Devices	The devices (drives and changer) to be used are listed. These are available on all endpoints. An endpoint is the logical target on the protection system to which the initiator connects.

Configure NTP

NTP is not part of the configuration wizard, but it is helpful to configure it after the completion of the configuration wizard to keep the protection system time synchronized with other systems in your environment.

Managing time and date settings

The Time and Date Settings tab enables you to view and configure the system time and date or configure the Network Time Protocol to set the time and date.

Before you begin

When using active directory mode for CIFS access, the system clock time can differ by no more than five minutes from that of the domain controller.

Procedure

1. To view the current time and date configuration, select **Administration** > **Settings** > **Time and Date Settings**.

   The Time and Date Settings page presents the current system date and time, shows whether NTP is enabled or not, and lists the IP addresses or host names of configured NTP servers.

2. To change the configuration, select **More Tasks** > **Configure Time Settings**.

   The Configure Time Settings dialog box appears.

3. In the **Time Zone** list, select the time zone where the system resides.
4. To manually set the time and date, select **None**, type the date in the **Date** box, and select the time in the **Time** lists.
5. To use NTP to synchronize the time, select NTP and set how the NTP server is accessed.
   - To use DHCP to automatically select a server, select **Obtain NTP Servers using DHCP**.
   - To configure an NTP server IP address, select **Manually Configure**, add the IP address of the server, and click **OK**.

   ⚠ WARNING When the system is configured for Active Directory authentication, it uses an alternate mechanism to sync time with the domain controller. To avoid time sync conflicts, do not enable NTP when the system is configured for Active Directory authentication.

6. Click **OK**.
7. If you changed the time zone, you must reboot the system:
   a. Select **Maintenance** > **System**.
   b. Click **Reboot System**.
   c. Click **OK** to confirm.

Command line interface

The command line interface (CLI) is a text-driven interface that can be used instead of or in addition to DD System Manager. Most management tasks can be performed in DD System Manager or with the CLI. In some cases, the CLI offers configuration options and reports that are not yet supported in DD System Manager.

Any protection system command that accepts a list, such as a list of IP addresses, accepts entries separated by commas, by spaces, or both.

The Tab key can be used to do the following.

- Complete a command entry when that entry is unique. Tab completion is supported for all keywords. For example, entering `syst` Tab `sh`Tab `st` Tab displays the command `system show stats`.
- Show the next available option, if you do not enter any characters before pressing the Tab key.
- Show partial matched tokens or complete a unique entry, if you enter characters before pressing the Tab key.

The *DD OS Command Reference Guide* provides information for each of the CLI commands. Online help is available and provides the complete syntax for each command.

Logging into the CLI

You can access the CLI by using a direct connection to the protection system or by using an Ethernet connection through SSH or Telnet. By default, SSH is enabled and Telnet is disabled.

Before you begin

To use the CLI, you must establish a local or remote connection to the protection system using one of the following methods.

- If you are connecting through a serial console port on the system, connect a terminal console to the port and use the communication settings: 115200 baud, 8 data bits, no parity, and 1 stop bit.

- If the system supports keyboard and monitor ports, connect a keyboard and monitor to those ports.
- If you are connecting through Ethernet, connect a computer with SSH or Telnet client software to an Ethernet network that can communicate with the system.

Procedure

1. If you are using an SSH or Telnet connection to access the CLI, start the SSH or Telnet client and specify the IP address or host name of the protection system.

   For information on initiating the connection, see the documentation for the client software. The system prompts you for a username.
2. When prompted, enter your protection system username or `sysadmin`, the default username.
3. When prompted, enter the password for the specified username.

The following example shows SSH login to a system named *mysystem* using SSH client software.

```
# ssh -l sysadmin mysystem.mydomain.com
 DD9900-157.dellemc.com
DD OS
Password:
```

CLI online help guidelines

The CLI displays two types of help: syntax-only help and command-description help, which includes the command syntax. Both types of help offer features that enable you reduce the time it takes to find the information you need.

The following guidelines describe how to use syntax-only help.

- To list the top-level CLI commands, enter a question mark (`?`), or type `help` or `man` at the prompt.
- To list all forms of a top-level command, enter the command with no options at the prompt or enter *command* `?`.
- To list all commands that use a specific keyword, enter `help` *keyword*, `man` *keyword*, or `?` *keyword*.
  For example, `? password` displays all system commands that use the password argument.

The following guidelines describe how to use command-description help.

- To list the top-level CLI commands, enter a question mark (`?`), or type `help` or `man` at the prompt.
- To list all forms of a top-level command with an introduction, enter `help` *command*, `man` *command*, or `?` *command*.
- The end of each help description is marked `END`. Press Enter to return to the CLI prompt.
- When the complete help description does not fit in the display, the colon prompt (`:`) appears at the bottom of the display. The following guidelines describe what you can do when this prompt appears.
  - To move through the help display, use the up and down arrow keys.

- To quit the current help display and return to the CLI prompt, press q.
- To display help for navigating the help display, press h.
- To search for text in the help display, enter a slash character (/) followed by a pattern to use as search criteria and press Enter. Matches are highlighted.

CHAPTER 3

Managing the Protection System

This chapter includes:

System management overview

DD System Manager allows you to manage the system on which DD System Manager is installed.

To support replication, DD System Manager supports the addition of systems running the previous two versions, the current version and the next two versions as they become available. DD System Manager supports the addition of systems up to two releases back as replication targets. The DD OS 7.0 release includes DD OS 6.2 and DD OS 6.1.

Note: When processing a heavy load, a system might be less responsive than normal. In this case, management commands issued from either DD System Manager or the CLI might take longer to complete. When the duration exceeds allowed limits, a timeout error is returned, even if the operation completed.

The following table lists the recommendations for the maximum number of user sessions supported by DD System Manager:

Table 23 Maximum number of users supported by DD System Manager

System Model	Maximum Active Users	Maximum Logged In Users
4 GB models[a]	5	10
16 GB and greater models[b]	10	20

a. Includes DD2200 (4 TB)
b. DD2200 (>7.5TB), DD6300, DD6800, DD6900, DD9300, DD9400, DD9500, DD9800, and DD9900

Note: Initial HA system set-up cannot be configured from the DD System Manager, but the status of a configured HA system can be viewed from DD System Manager.

HA system management overview

The HA relationship between the two nodes, one active and one standby, is setup through DD OS CLI commands.

Initial set-up can be run on either of the two nodes but only one at a time. It is a requirement for HA that the system interconnect and identical hardware is setup on both nodes first.

Note: Both nodes of the HA pair are required to have identical hardware. This requirement is validated during setup and system boot-up.

When configuring HA for the first time, the `ha create` command needs to be run on the node with the license installed. To upgrade an existing system to HA by adding and a new or unconfigured system, initiate the HA upgrade from the existing standalone system.

HA system planned maintenance

The HA architecture provides a rolling upgrade, which reduces maintenance downtime for the upgrade.

With a rolling upgrade, the HA nodes are upgraded one at a time. The standby node is rebooted and upgraded first. The newly upgraded standby node then takes over the active role through an HA failover. After the failover, the second node is rebooted and assumes the role of the standby node after the upgrade.

System upgrade operations that require data conversion cannot start until both systems are upgraded to the same level and HA state is fully restored.

Restarting a protection system

You may be required to restart a protection system after modifying the configuration for the change to take effect. For example, changing the time zone requires that you restart the system before the new time zone is applied.

About this task

Procedure

1. Select **Maintenance** > **System** > **Reboot System**.
2. Click **OK** to confirm.

Powering a protection system on or off

When powering a protection system off and on, it is important that you follow the proper procedure to preserve the file system and configuration integrity.

About this task

Do not use the chassis power switch or the IMPI Remote System Power Down feature to power off the protection system unless the `system poweroff` command is unsuccessful. Using the chassis power switch to power down the system prevents remote power control using IPMI. Using the IMPI Remote System Power Down feature to power off the protection system does not perform an orderly shutdown.

For HA systems, a management connection to both nodes is required.

Complete the following steps to power off a protection system.

Procedure

1. Verify that I/O on the system is stopped.

   Run the following commands:

   - `cifs show active`
   - `nfs show active`
   - `system show stats view sysstat interval 2`
   - `system show perf`

2. For HA systems, verify the health of the HA configuration.

   Run the following command:

   ```
   ha status
   ```

   ```
   HA System Name: dd9900-ha3a.example.com
   HA System Status: highly available
   Node Name                  Node ID   Role      HA State
   -------------------------- --------- --------- --------
   dd9900-ha3a-p0.example.com   0       active    online
   dd9900-ha3a-p1.example.com   1       standby   online
   -------------------------- --------- --------- --------
   ```

   Note: This output sample is from a healthy system. If the system is being shut down to replace a failed component, the HA System Status will be degraded, and one or both nodes will show offline for the HA State.

3. Run the `alerts show current` command. For HA pairs, run the command on the active node first, and then the standby node.

4. For HA systems, run the `ha offline` command if the system is in a highly available state with both nodes online. Skip this step if the HA status is degraded.
5. Run the `system poweroff` command. For HA pairs, run the command on the active node first, and then the standby node.

   ```
   # system poweroff

   Continue? (yes|no|?) [no]: yes
   ```
6. Remove the power cords from the power supplies on the controller or controllers.
7. Verify that the blue power LED is off on the controllers to confirm that the system is powered down.

   Once the controller is powered off, switch off any external expansion shelves (ES30, DS60, FS15).

Power a protection system on

About this task

Restore power to the protection system when the system downtime is complete.

Procedure

1. Power on any expansion shelves before powering on the controller. Wait approximately three minutes after all expansion shelves are turned on.

   Note: A controller is the chassis and any internal storage. A protection system refers to the controller and any external storage.

2. Plug in the power cord for your controller, and if there is a power button on the controller, press the power button, as shown in the *Installation Guide* for your system. For HA systems, power on the active node first, and then the standby node.

   Note: Some protection system appliances do not have a traditional power button, and are designed to be "always on." These devices will power up as soon as AC power is applied.

3. For HA systems, verify the health of the HA configuration.

   Run the following command:
   `ha status`

   ```
   HA System Name: dd9900-ha3a.example.com
   HA System Status: highly available
   Node Name                  Node ID   Role      HA State
   -------------------------- --------- --------- --------
   dd9900-ha3a-p0.example.com   0       active    online
   dd9900-ha3a-p1.example.com   1       standby   offline
   -------------------------- --------- --------- --------
   ```
4. For HA systems, if one of the nodes displays as offline, run the `ha online` command on that node to restore the HA configuration.
5. Verify the system is fully booted and the operating system is running. This can be done through a serial connection or from an SSH session to the system. The system is up when you can log into the system.
6. Run the `alerts show current` command. For HA pairs, run the command on the active node first, and then on the standby node.

System upgrade management

To upgrade a DD OS system, you must verify that there is sufficient room for the new software on the target system. Transfer the software to the system to be upgraded, and then start the upgrade.

If the system uses MD5-signed certificates, regenerate the certificates with a stronger hash algorithm during the upgrade process.

HA system upgrades

For an HA system, transfer the software to the active node and start the upgrade from the active node. Use the floating IP address to access DD System Manager to perform software upgrades. The upgrade process on an HA system automatically upgrades both the active and standby nodes.

Minimally disruptive upgrade

The minimally disruptive upgrade (MDU) feature lets you upgrade specific software components or apply bug fixes without needing to perform a system reboot. Only those services that depend on the component being upgraded are disrupted, so the MDU feature can prevent significant downtime during certain software upgrades.

Not all software components qualify for an MDU; such components must be upgraded as part of a regular DD OS system software upgrade. A DD OS software upgrade uses a large RPM (upgrade bundle), which performs upgrade actions for all of the components of DD OS. MDU uses smaller component bundles, which upgrade specific software components individually, which makes the MDU RPM much smaller than a full DD OS RPM.

Contact Support to determine if an MDU is available for a specific issue.

RPM signature verification

RPM signature verification validates DD OS RPMs that you download for upgrade. If the RPM has not been tampered with, the digital signature is valid and you can use the RPM as usual. If the RPM has been tampered with, the corruption invalidates the digital signature, and the RPM is rejected by DD OS. An appropriate error message is displayed.

The signatures are SHA1 or MD5.

Support software

DD OS 6.1 introduced a type of software package called support software for instances where the software packages must be signed in order to use it for the DD OS upgrade. Support software is an MDU package created and signed by Support Engineering to address specific issues. By default, the protection system does not allow support software to be installed on the system. Contact Support for more information about support software.

Pre-upgrade checklists and overview

Review the items in these checklists before performing any DD OS upgrade. Doing so can simplify the upgrade process and minimize potential difficulties.

Pre-upgrade manual tasks

CAUTION Failure to perform the tasks in this section may result in an upgrade failure.

These are tasks that you should plan to do prior to the upgrade. These tasks are not performed automatically by any process.

1. Reboot the system. For HA systems, follow the reboot instructions described in Upgrade considerations for HA systems on page 57 after performing the rest of the checks in this section.
2. Check for current alerts; this can reveal many such disk and other hardware failures that should be addressed prior to upgrading:

   ```
   # alert show current
   ```
3. Verify the system network configuration:

   ```
   # net show config
   ```

   ```
   # net show hardware
   ```
4. Check whether all network interfaces are up and have appropriate IP addresses:

   ```
   # net show settings
   ```
5. Check the disk states, and do not perform the upgrade if the system is low on spares or has disks that show in the absent, failed, or reconstructing states:

   ```
   # disk show state
   ```
6. Check the disk reliability, and replace any disks that have more than 50 reallocated sectors:

   ```
   # disk show reliability-data
   ```
7. Check the enclosure status:

   ```
   # enclosure show all
   ```

   It should say "OK" for all devices.
8. Check whether the enclosure topology is correct:

   ```
   # enclosure show topology
   ```

   Also check whether any error appears with an asterisk (*) next to the **enc.ctrl.port** field. Also check the **Error Message** field for any errors such as "A possible problem was detected for this shelf controller or the cable connected to it."
9. Check that the device port mapping is correct:

   ```
   # system show hardware
   ```
10. Check the link speed for connected ports:

    ```
    # system show ports
    ```
11. Check the status of the file system to determine that file system is enabled and running normally:

    ```
    # filesys status
    ```
12. Check if file system cleaning is running, and if so, stop it:

    ```
    # filesys clean status
    ```

    ```
    # filesys clean stop
    ```
13. If replication is enabled, check its status:

    ```
    # replication status
    ```
14. For a system enabled with Cloud Tier, ensure there is no data movement:

    ```
    # data-movement status
    ```

    ```
    # data-movement stop all
    ```
15. Check if cloud cleaning is running, and if so, stop it:

```
# cloud clean status
```

```
# cloud clean stop
```

16. Check if any backup and restore activity is in progress, and if so, stop it:

```
# system show stats
```

17. Run an Autosupport Report just prior to performing the DD OS upgrade to determine if the system reports errors that need to be resolved before the upgrade:

```
# autosupport send <your_email_address>
```

18. If the Autosupport Report indicated issues with the system, check `kern.info` log, and if you notice frequent failures in hardware, contact Support to inspect your system before you perform the upgrade.

```
# log view debug/platform/kern.info
```

Search for the string `ERROR` in the log file.

Upgrade considerations for HA systems

HA systems require some unique steps before initiating the upgrade operation, and one unique post-check after the upgrade is complete.

CAUTION Perform the manual checks described in Pre-upgrade manual tasks on page 55 before rebooting the HA system.

When upgrading an HA system, upload the upgrade RPM package to the active node.

1. The HA system must be in a highly available state, with both nodes online before performing the DD OS upgrade. Run the `ha status` command to verify the HA system state.

```
# ha status
HA System Name: dd9900-ha3a.example.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
dd9900-ha3a-p0.example.com   0       active    online
dd9900-ha3a-p1.example.com   1       standby   online
-------------------------- --------- --------- --------
```

2. Reboot the standby node (node 1).
3. Run the `ha status` command to verify the HA system status displays as `highly available` after the standby node reboots.
4. Run the `ha failover` command to initiate a failover from the active node to the standby node.
5. Run the `ha status` command to verify node 1 is the active node and node 0 is the standby node.

```
# ha status
HA System Name: dd9900-ha3a.example.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
dd9900-ha3a-p0.example.com   0       standby   online
dd9900-ha3a-p1.example.com   1       active    online
-------------------------- --------- --------- --------
```

6. Reboot the standby node (node 0).
7. Run the `ha status` command to verify the HA system status displays as `highly available` after the standby node reboots.
8. Run the `ha failover` command to initiate a failover from the active node to the standby node.

9. Run the `ha status` command to verify the node 0 is the active node and node 1 is the standby node.

```
# ha status
HA System Name: dd9900-ha3a.example.com
HA System Status: highly available
Node Name                  Node ID   Role      HA State
-------------------------- --------- --------- --------
dd9900-ha3a-p0.example.com   0       active    online
dd9900-ha3a-p1.example.com   1       standby   online
-------------------------- --------- --------- --------
```

Initiate the upgrade from the active node. DD OS automatically recognizes the HA system and performs the upgrade procedure on both nodes. The HA upgrade runs in the following sequence:

1. The standby node is upgraded first, then reboots.
2. After the reboot is complete, the HA system initiates a failover and the standby node takes over as the active node.
3. The original active node is upgraded, then reboots and remains as the standby node.

After both nodes are upgraded, the system does not perform another failover to return the nodes to their original configuration.

After the upgrade procedure is complete, run the `ha status` command again to verify that the system is in a highly available state, and both nodes are online.

Optionally run the `ha failover` command to return the nodes to the roles they were in before the upgrade.

Automatic tasks performed prior to the upgrade

Understanding these aspects of a DD OS upgrade assures a smoother process.

DD OS performs these tasks before a system upgrade:

1. Determines whether replication initialization is in progress. If it is, the upgrade does not proceed.
2. Inspects all the digests and signatures that are contained in `.rpm` file to ensure the integrity and origin of the package. If the signature is not valid, the upgrade does not proceed.
3. Determines whether the upgrade from the old version of DD OS to the new one is permissible. Systems running DD OS 6.1.X. or 6.2.X can upgrade directly to 7.0. This restriction is due to the RPM signing. An upgrade is not permitted under these circumstances:
   a. The upgrade target is the same version as the software already running on the system.
   b. Reverting to a prior release is not allowed, such as from 7.0.0.5 to 6.2.0.10
   c. The upgrade exceeds two feature families, such as from 6.0 to 7.0.
4. Determines whether any NFS mount points are unknown. If any NFS mount points are unknown, the upgrade does not proceed.
5. Determines whether the previous upgrade, if any, completed successfully. If the previous upgrade was unsuccessful or did not complete, the current upgrade does not proceed.

Automatic tasks performed by the upgrade script (in the .rpm file) prior to upgrade

These tests precede the actual system upgrade process. The system:

1. Determines whether two different kinds of NVRAM cards are present.
2. Checks the `/ddr` partition and `/` (root) partition sizes for space utilization.
3. Checks the OST version.
4. Determines whether the RAID metagroup is assembled. If it is not assembled, the upgrade process does not begin.

5. Determines available space for the file system.
6. Determines whether sufficient space is available for the upgrade.
7. Checks the VTL version, if VTL is present.
8. Determines whether the file system is enabled, and if it is not enabled, enable it.
9. Determines whether VTL is enabled.
10. Checks the VTL pools to insure that they can be converted to MTrees.
11. Determines whether sufficient VTL space is available.
12. Ensures that the numbers of MTrees and VTL pools do not exceed 100.
13. Determines whether all dg0 disks are located on head unit. If not, the upgrade process does not begin, and the problem must be addressed.
14. Determines whether the file system can be shutdown without problems. If the file system cannot be shut down in a clean manner, the upgrade process will stop.

The upgrade process quits if it encounters a failure in any of the tasks listed.

Conditions that prevent the upgrade process

Several conditions can cause the upgrade process to be stopped:

- The system is not in a functional state. For example:
  - Storage is functionally deficient, such as an enclosure is missing.
  - The file system did not shutdown cleanly, resulting in a core dump.
  - The previous upgrade did not complete correctly.
- Space usage is problematic. For example:
  - The / (root) or `/ddr` partition is full with log files, core dumps, and so forth.
  - Insufficient storage space is available to perform the data upgrade.
- The system is not configured correctly. For example, NFS mount points were manually created under root.
- Features are incompatible between the original and target versions of DD OS:
  - DD OS versions 7.0 and later do not support DD Extended Retention. Any system with DD Extended Retention enabled cannot be upgraded to DD OS 7.0. Migrate the data to a system running DD OS 6.1.X or 6.2.X without DD Extended Retention running. After the migration, upgrade the DD OS 6.1.X or 6.2.X system without DD Extended Retention to DD OS 7.0.
  - DD OS versions 7.0 and later do not support the RSA key manager for data at rest encryption. If a DD OS 6.X system uses the RSA key manager for data at rest encryption, upgrades to DD OS 7.0 and later are not permitted. Disable data at rest encryption to proceed with the DD OS upgrade.

The goal of checking these conditions is to prevent any upgrade problems or file system anomalies to occur or propagate. The conditions are also applied in upgrades involving source and destination partner systems in replication.

Note: For security reasons, there is a 30-minute time limit for the upload of RPM packages for DDMC and DD system upgrades using the DDMC GUI. If you have a slow connection from a client machine to the DDMC and the upload takes more than 30 minutes, the connection drops and you cannot use DDMC to upload the package.
Workaround: Use the CLI to upload the package into DDMC (for example, use `SCP/PSCP` from a Unix terminal or Windows CMD).

For DDMC upgrades, upload the package to `/ddr/var/releases`.

For DD System upgrades, upload the package to `/ddr/var/ddr-releases`.

Viewing upgrade packages on the protection system

DD System Manager allows you to view and manage up to five upgrade packages on a protection system. Before you can upgrade a system, you must download an upgrade package from the Online Support site to a local computer, and then upload it to the target system.

Procedure

1. Select **Maintenance** > **System**.
2. Optionally, select an upgrade package and click **View Checksum** to display the MD5 and SHA256 checksums of the upgrade package.

Results

For every package stored on the system, DD System Manager displays the filename, file size, and last modified date in the list titled: Upgrade Packages Available on *<protection system>*.

Obtaining and verifying upgrade packages

Use the DD System Manager to open a session with the Dell EMC Online Support site to select an upgrade package for download.

About this task

Note: You can use FTP, NFS, or SCP to copy an upgrade package to a system. DD System Manager can manage up to 5 system upgrade packages. This limitation does not apply if you manage system upgrade packages through a network share linked to the `/ddvar/releases` directory on the protection system. There are no restrictions, other than space limitations, when you manage the files directly in the `/ddvar/releases` directory. FTP is disabled by default. To use NFS, `/ddvar` needs to be exported and mounted from an external host).

Procedure

1. Select **Maintenance** > **System**.
2. To obtain an upgrade package, click the **Dell EMC Online Support** link, click Downloads, and use the search function to locate the package recommended for your system by Support personnel. Save the upgrade package to the local computer.
3. Verify that there are no more than four packages listed in the Upgrade Packages Available on *<protection system>* list.

   DD System Manager can manage up to five upgrade packages. If five packages appear in the list, remove at least one package before uploading the new package.
4. Click **Upload Upgrade Package** to initiate the transfer of the upgrade package to the protection system.
5. In the **Upload Upgrade Package** dialog box, click **Browse** to open the **Choose File to Upload** dialog box. Navigate to the folder with the downloaded file, select the file, and click **Open**.
6. Click **OK**.

   An upload progress dialog box appears. Upon successful completion of the upload, the download file (with a .rpm extension) appears in the list titled: Upgrade Packages Available on *<protection system>*.

7. To verify the upgrade package integrity, click **View Checksum** and compare the calculated checksum displayed in the dialog box to the authoritative checksum on the Online Support site.
8. To manually initiate an upgrade precheck, select an upgrade package and click **Upgrade Precheck**.

Upgrading a protection system

When an upgrade package file is present on a protection system, you can use DD System Manager to perform an upgrade using that upgrade package.

Before you begin

Read the DD OS Release Notes for the complete upgrade instructions and coverage of all the issues that can impact the upgrade.

About this task

The procedure that follows describes how to initiate an upgrade using DD System Manager. Log out of any CLI sessions on the system where the upgrade is to be performed before using DD System Manager to upgrade the system.

Note: Upgrade package files use the .rpm file extension. This topic assumes that you are updating only DD OS. If you make hardware changes, such as adding, swapping, or moving interface cards, you must update the DD OS configuration to correspond with the hardware changes.

Procedure

1. Log into DD System Manager on the protection system where the upgrade is to be performed.

   Note: As recommended in the Release Notes, reboot the protection system before upgrading to verify that the hardware is in a clean state. If any issues are discovered during the reboot, resolve those issues before starting the upgrade. For an MDU upgrade, a reboot might not be needed.

2. Select **Maintenance** > **System**.
3. From the **Upgrade Packages Available on *<protection system>*** list, select the package to use for the upgrade.

   Note: You must select an upgrade package for a newer version of DD OS. DD OS does not support downgrades to previous versions.

4. Click **Perform System Upgrade**.

   The **System Upgrade** dialog box appears and displays information about the upgrade and a list of users who are currently logged in to the system to be upgraded.

5. Verify the version of the upgrade package, and click **OK** to continue with the upgrade.

   The **System Upgrade** dialog box displays the upgrade status and the time remaining.

   When upgrading the system, you must wait for the upgrade to complete before using DD System Manager to manage the system. If the system restarts, the upgrade might continue after the restart, and DD System Manager displays the upgrade status after login. If possible, keep the System Upgrade progress dialog box open until the upgrade completes or the system restarts. A Login link appears when the upgrade is complete.

   Note: To view the status of an upgrade using the CLI, enter the `system upgrade status` command. Log messages for the upgrade are stored in `/ddvar/log/debug/`

`platform/upgrade-error.log` and `/ddvar/log/debug/platform/upgrade-info.log`.

6. If the system powers down, you must remove AC power from the system to clear the prior configuration. Unplug all power cables for 30 seconds, and then plug them back in. The system powers on and restarts.
7. If the system does not automatically power on and there is a power button on the front panel, press the button.

After you finish

The following requirements may apply after completing an upgrade.

- For environments that use self-signed SHA-256 certificates, the certificates must be regenerated manually after the upgrade process is complete and trust must be re-established with external systems that connect to the protection system.
  1. Run the `adminaccess certificate generate self-signed-cert regenerate-ca` command to regenerate the self-signed CA and host certificates. Regenerating the certificates breaks existing trust relationships with external systems.
  2. Run the `adminaccess trust add host hostname type mutual` command to reestablish mutual trust between the protection system and the external system.
- If the system shows existing or configured FC ports with missing WWPN or WWNN information, or reports that no FC host bus adapter (HBA) driver is installed, run the `scsitarget endpoint enable all` command.

Replication notes

With collection replication, no files are visible on the destination system if replication was not finished before starting the upgrade. After the upgrade, wait until replication completes to see files on the destination system.

Removing an upgrade package

A maximum of five upgrade packages can be uploaded to a protection system with DD System Manager. If the system you are upgrading contains five upgrade packages, you must remove at least one package before you can upgrade the system.

About this task

Procedure

1. Select **Maintenance** > **System**.
2. From the list titled **Upgrade Packages Available on *<protection system>***, select the package to remove. One package can be removed at a time.
3. Click **Remove Upgrade Package**.

Managing electronic licenses

Add and delete electronic licenses from the system. Refer to the applicable Release Notes for the most up-to-date information on product features, software updates, software compatibility guides, and information about products, licensing, and service. If DD Retention Lock Compliance is enabled on the system, the `elicense` CLI commands are required to update or remove licenses because license control in the DD SM GUI is disabled.

HA system license management

HA is a licensed feature, and the system licensing key is registered by following the steps to add any other license to the DD system.

A system is configured as Active-Standby, where one node is designated "standby." Only one set of licenses is required for both nodes. During failover, the licenses on one node will failover to the other node.

Protection system storage management

System storage management features enable you to view the status and configuration of your storage space, flash a disk LED to facilitate disk identification, and change the storage configuration.

Note: All storage that is connected or used by the two-node Active-Standby HA system can be viewed as a single system.

Using the CLI to calculate usable storage space

The following values are required to calculate the usable storage on a protection system after accounting for RAID overhead:

- *N*= Number of disks in use in the disk group (dg).
- *C* = Capacity of each disk after formatting.
- *R* = 2 (Number of disks used for RAID 6 parity)

This calculation does not work for Cache Tier storage, because the Cache Tier disks are not RAID protected.

Run the `storage show all` command to get the values for *N* and *C*.

Figure 4 Example of `storage show all` command

```
sysadmin@ddbeta90# storage show all
Active tier details:
Disk       Disks       Count   Disk        Additional
Group                          Size        Information
-------    --------    -----   --------    -----------
dg2        2.1-2.14    14      2.7 TiB
(spare)    2.15        1       2.7 TiB
-------    --------    -----   --------    -----------

Current active tier size: 32.7 TiB
Active tier maximum capacity: 131.0 TiB
```

In this example there are 14 disks in use in dg2 and each disk has a capacity of 2.7 TiB, therefore *N*=14 and *C*= 2.7 TiB

Use the formula (*N*-*R*) x *C* to get the usable capacity. In this example, the equation is (14-2) x 2.7 TiB.

12 x 2.7 TiB = 32.4 TiB, or 35.6 TB.

Note: The calculated value may not match exactly with the output of the `storage show all` command due to the way the capacity values are rounded for display. The `disk show hardware` command displays the disk capacity with additional decimal places.

Viewing system storage information

The storage status area shows the current status of the storage, such as Operational or Non-Operational, and the storage migration status. Below the Status area are tabs that organize how the storage inventory is presented.

Procedure

1. To display the storage status, select **Hardware** > **Storage**.
2. If an alerts link appears after the storage status, click the link to view the storage alerts.
3. If the Storage Migration Status is Not licensed, you can click **Add License** to add the license for this feature.

Overview tab

The Overview tab displays information for all disks in the protection system organized by type. The categories that display are dependent on the type of storage configuration in use.

The Overview tab lists the discovered storage in one or more of the following sections.

- Active Tier
  Disks in the Active Tier are currently marked as usable by the file system. Disks are listed in two tables, Disks in Use and Disks Not in Use.
- Cache Tier
  SSDs in the Cache Tier are used for caching metadata. The SSDs are not usable by the file system. Disks are listed in two tables, Disks in Use and Disks Not in Use.
- Cloud Tier
  Disks in the Cloud Tier are used to store the metadata for data that resides in cloud storage. The disks are not usable by the file system. Disks are listed in two tables, Disks in Use and Disks Not in Use.
- Addable Storage
  For systems with optional enclosures, this section shows the disks and enclosures that can be added to the system.
- Failed/Foreign/Absent Disks (Excluding Systems Disks)
  Shows the disks that are in a failed state; these cannot be added to the system Active or Retention tiers.
- Systems Disks
  Shows the disks where the DD OS resides when the protection system controller does not contain data storage disks.
- Migration History
  Shows the history of migrations.

Each section heading displays a summary of the storage configured for that section. The summary shows tallies for the total number of disks, disks in use, spare disks, reconstructing spare disks, available disks, and known disks.

Click a section plus (+) button to display detailed information, or click the minus (-) button to hide the detailed information.

Table 24 Disks In Use column label descriptions

Item	Description
Disk Group	The name of the disk group that was created by the file system (for example, dg1).

Table 24 Disks in Use column label descriptions (continued)

Item	Description
State	The status of the disk (for example Normal, Warning).
Disks Reconstructing	The disks that are undergoing reconstruction, by disk ID (for example, 1.11).
Total Disks	The total number of usable disks (for example, 14).
Disks	The disk IDs of the usable disks (for example, 2.1-2.14).
Size	The size of the disk group (for example, 25.47 TiB).

Table 25 Disks Not in Use column label descriptions

Item	Description
Disk	The disk identifier, which can be any of the following. • The enclosure and disk number (in the form Enclosure Slot) • A device number for a logical device such as those used by DD VTL and vDisk • A LUN
Slot	The enclosure where the disk is located.
Pack	The disk pack, 1–4, within the enclosure where the disk is located. This value will only be 2-4 for DS60 expansion shelves.
State	The status of the disk, for example In Use, Available, Spare.
Size	The data storage capacity of the disk.[a]
Type	The disk connectivity and type (For example, SAS).

a. The DD OS convention for computing disk space defines one gibibyte as 230 bytes, giving a different disk capacity than the manufacturer's rating.

Enclosures tab

The Enclosures tab displays a table summarizing the details of the enclosures connected to the system.

The Enclosures tab provides the following details.

Table 26 Enclosures tab column label descriptions

Item	Description
Enclosure	The enclosure number. Enclosure 1 is the head unit.
Serial Number	The enclosure serial number.
Disks	The disks contained in the enclosure, in the format *<Enclosure-number>*.1-*<Enclosure-number>*.*<N>*.
Model	The enclosure model. For enclosure 1, the model is Head Unit.
Disk Count	The number of disks in the enclosure.

Table 26 Enclosures tab column label descriptions (continued)

Item	Description
Disk Size	The data storage capacity of the disk.[a]
Failed Disks	The failed disks in the enclosure.
Temperature Status	The temperature status of the enclosure.

a. The DD OS convention for computing disk space defines one gibibyte as 230 bytes, giving a different disk capacity than the manufacturer's rating.

Disks tab

The Disks tab displays information on each of the system disks. You can filter the disks viewed to display all disks, disks in a specific tier, or disks in a specific group.

The Disk State table displays a summary status table showing the state of all system disks.

Table 27 Disks State table column label descriptions

Item	Description
Total	The total number of inventoried disks.
In Use	The number of disks currently in use by the file system.
Spare	The number of spare disks (available to replace failed disks).
Spare (reconstructing)	The number of disks that are in the process of data reconstruction (spare disks replacing failed disks).
Available	The number of disks that are available for allocation to the Active storage tier.
Known	The number of known unallocated disks.
Unknown	The number of unknown unallocated disks.
Failed	The number of failed disks.
Foreign	The number of foreign disks.
Absent	The number of absent disks.
Migrating	The number of disks serving as the source of a storage migration.
Destination	The number of disks serving as the destination of a storage migration.
Powered Off	The number of disks not powered on.
Not Installed	The number of empty disk slots that the system can detect.

The Disks table displays specific information about each disk installed in the system.

Table 28 Disks table column label descriptions

Item	Description
Disk	The disk identifier, which can be:

Table 28 Disks table column label descriptions (continued)

Item	Description
	• The enclosure and disk number (in the form *Enclosure.Slot*). • A device number for a logical device such as those used by DD VTL and vDisk.. • A LUN.
Size	The size of the disk.
Slot	The enclosure where the disk is located.
Pack	The disk pack, 1-4, within the enclosure where the disk is located. This value will only be 2-4 for DS60 expansion shelves.
State	The status of the disk, which can be one of the following. • Absent. No disk is installed in the indicated location. • Available. An available disk is allocated to the active or retention tier, but it is not currently in use. • Copy Recovery. The disk has a high error rate but is not failed. RAID is currently copying the contents onto a spare drive and will fail the drive once the copy reconstruction is complete. • Destination. The disk is in use as the destination for storage migration. • Error. The disk has a high error rate but is not failed. The disk is in the queue for copy reconstruction. The state will change to Copy Recovery when copy reconstruction begins. • Foreign. The disk data indicates the disk may be owned by another system, and the disk cannot be assigned to a tier until it is in the Unknown state. • In-Use. The disk is being used for backup data storage. • Known. The disk is a supported disk that is ready for allocation. • Migrating. The disk is in use as the source for storage migration. • Powered Off. The disk power has been removed by Support. • Reconstruction. The disk is reconstructing in response to a `disk fail` command or by direction from RAID/SSM. • Spare. The disk is available for use as a spare. • System. System disks store DD OS and system data. No backup data is stored on system disks. • Unknown. An unknown disk is not allocated to the active or retention tier. It might have been failed administratively or by the RAID system.

Table 28 Disks table column label descriptions (continued)

Item	Description
Manufacturer/Model	The manufacturer's model designation. The display may include a model ID or RAID type or other information depending on the vendor string sent by the storage array.
Firmware	The firmware level used by the third-party physical-disk storage controller.
Serial Number	The manufacturer's serial number for the disk.
Disk Life Used	The percentage of an SSD's rated life span consumed.
Type	The disk connectivity and type (For example, SAS).

Reconstruction tab

The Reconstruction tab displays a table that provides additional information on reconstructing disks.

The following table describes the entries in the Reconstruction table.

Table 29 Reconstruction table column label descriptions

Item	Description
Disk	Identifies disks that are being reconstructed. Disk labels are of the format *enclosure.disk*. Enclosure 1 is the system controller, and external shelves start numbering with enclosure 2. For example, the label *3.4* is the fourth disk in the second shelf.
Disk Group	Shows the RAID group (dg#) for the reconstructing disk.
Slot	The enclosure where the reconstructing disk is located.
Tier	The name of the tier where the failed disk is being reconstructed.
Time Remaining	The amount of time before the reconstruction is complete.
Percent Complete	The percentage of reconstruction that is complete.

When a spare disk is available, the file system automatically replaces a failed disk with a spare and begins the reconstruction process to integrate the spare into the RAID disk group. The disk use displays `Spare` and the status becomes `Reconstructing`. Reconstruction is performed on one disk at a time.

Physically locating an enclosure

If you have trouble determining which physical enclosure corresponds to an enclosure displayed in DD System Manager, you can use the CLI beacon feature to flash the enclosure IDENT LEDs and all the disk LEDs that indicate normal operation.

Procedure

1. Establish a CLI session with the system.
2. Type `enclosure beacon` *enclosure*.
3. Press `Ctrl-C` to stop the LED flashing.

Physically locating a disk

If you have trouble determining which physical disk corresponds to a disk displayed in DD System Manager, you can use the beacon feature to flash an LED on the physical disk.

Procedure

1. Select **Hardware** > **Storage** > **Disks**.
2. Select a disk from the **Disks** table and click **Beacon**.

   Note: You can select one disk at a time.

   The Beaconing Disk dialog box appears, and the LED light on the disk begins flashing.
3. Click **Stop** to stop the LED beaconing.

Configuring storage

Storage configuration features allow you to add and remove storage expansion enclosures from the active, retention, and cloud tiers. Storage in an expansion enclosure (which is sometimes called an expansion shelf) is not available for use until it is added to a tier.

About this task

Note: Additional storage requires the appropriate license or licenses and sufficient memory to support the new storage capacity. Error messages display if more licenses or memory is needed.

DD6300 systems support the option to use ES30 enclosures with 4 TB drives (43.6 TiB) at 50% utilization (21.8 TiB) in the active tier if the available licensed capacity is exactly 21.8 TiB. The following guidelines apply to using partial capacity shelves:

- No other enclosure types or drive sizes are supported for use at partial capacity.
- A partial shelf can only exist in the Active tier.
- Only one partial ES30 can exist in the Active tier.
- Once a partial shelf exists in a tier, no additional ES30s can be configured in that tier until the partial shelf is added at full capacity.

  Note: This requires licensing enough additional capacity to use the remaining 21.8 TiB of the partial shelf.
- If the available capacity exceeds 21.8 TB, a partial shelf cannot be added.
- Deleting a 21 TiB license will not automatically convert a fully-used shelf to a partial shelf. The shelf must be removed, and added back as a partial shelf.

For DD6900, DD9400, and DD9900 systems, storage capacity licenses are available in increments of 60 TB raw (48 TB usable) capacity. Therefore, systems with 8 TB drives may encounter situations where the licensed capacity does not the full capacity of the disks installed in the disk shelves. For example, if a system has a licensed capacity of 48 TB usable capacity, and has one pack of 8 TB disks for a total of 96 TB usable capacity, only half the system capacity is available for use.

Procedure

1. Select **Hardware** > **Storage** > **Overview**.
2. Expand the dialog box for one of the available storage tiers:
   - **Active Tier**
   - **Cache Tier**

- **Cloud Tier**

3. Click **Configure**.
4. In the Configure Storage dialog box, select the storage to be added from the **Addable Storage** list.
5. In the **Configure** list, select **Active Tier**.

   The maximum amount of storage that can be added to the active tier depends on the DD controller used.

   Note: The licensed capacity bar shows the portion of licensed capacity (used and remaining) for the installed enclosures.

6. Select the checkbox for the Shelf to be added.
7. Click the **Add to Tier** button.
8. Click **OK** to add the storage.

   Note: To remove an added shelf, select it in the Tier Configuration list, click **Remove from Configuration**, and click **OK**.

DD3300 capacity expansion

The DD3300 system is available in four different capacity configurations. Capacity expansions from one configuration to another are supported.

The DD3300 system is available in the following capacity configurations:

- 4 TB
- 8 TB
- 16 TB
- 32 TB

The following upgrade considerations apply:

- A 4 TB system can be upgraded to 16 TB.
- An 8 TB can be upgraded to 16 TB, and from 16 TB to 32 TB.
- A 16 TB system can be upgraded to 32 TB.
- There is no upgrade path from 4 TB to 32 TB.

Select **Maintenance** > **System** to access information about capacity expansion, and to initiate the capacity expansion process.

The capacity expansion is a one-time process. The **Capacity Expansion History** pane displays whether the system has already been expanded. If the system has not been expanded, click the **Capacity Expand** button to initiate the capacity expansion.

All capacity expansions require the installation of additional disks and memory in the system. Do not attempt to expand the capacity until the hardware upgrades are complete. The following table lists the hardware upgrade requirements for capacity expansion.

Table 30 DD3300 upgrade requirements for capacity expansion

Capacity expansion	Additional memory	Additional HDDs	Additional SSD
4 TB to 16 TB	32 GB	6 x 4 TB HDDs	1 x 480 GB SSD

Table 30 DD3300 upgrade requirements for capacity expansion (continued)

Capacity expansion	Additional memory	Additional HDDs	Additional SSD
8 TB to 16 TB	8 TB to 16 TB expansion requires licensing and configuration changes only. No hardware upgrades are required.		
16 TB to 32 TB	16 GB	6 x 4 TB HDDs	N/A

The *DD3300 Field Replacement and Upgrade Guide* provides detailed instructions for expanding system capacity.

Capacity Expand

Select the target capacity from the **Select Capacity** drop-down list. A capacity expansion can be prevented by insufficient memory, insufficient physical capacity (HDDs), the system has already been expanded, or the target for capacity expansion is not supported. If the capacity expansion cannot be completed, the reason will display here.

Capacity expansion history

The **Capactiy Expansion History** table displays details about the capacity of the system. The table provides the capacity of the system when the software was first installed, the date of the initial software installation. If the capacity was expanded, the table also provides the expanded capacity, and the date the expansion was performed.

Fail and unfail disks

Disk fail functionality allows you to manually set a disk to a failed state to force reconstruction of the data stored on the disk. Disk unfail functionality allows you to take a disk in a failed state and return it to operation.

Fail a disk

Fail a disk and force reconstruction. Select **Hardware** > **Storage** > **Disks** > **Fail**.

Select a disk from the table and click **Fail**.

Unfail a disk

Make a disk previously marked Failed or Foreign usable to the system. Select **Hardware** > **Storage** > **Disks** > **Unfail**.

Select a disk from the table and click **Unfail**.

Network connection management

Network connection management features allow you view and configure network interfaces, general network settings, and network routes.

HA system network connection management

The HA system relies on two different types of IP addresses, fixed and floating. Each type has specific behaviors and limitations.

On an HA system, Fixed IP addresses:

- Are used for node management via the CLI
- Are attached ("fixed") to the node
- Can be static or DHCP, IPv6 SLAAC, and IPv6 Linklocal

  Note: SLAAC and Linklocal are auto-generated address that appear when the interface is in a running state. Users have no control over these addresses, but they are available to transfer data.
- Configuration is done on the specific node with the `type fixed` argument

Note: All file system access should be through a floating IP.

Floating IP addresses only exist in the two-node HA system; during failover, the IP address "float" to the new active node and are:

- Only configured on the active node
- Used for filesystem access and most configuration
- Can only be static
- Configuration requires the `type floating` argument

Network interface management

Network interface management features enable you to manage the physical interfaces that connect the system to a network and create logical interfaces to support link aggregation, load balancing, and link or node failover.

Viewing interface information

The Interfaces tab enables you to manage physical and virtual interfaces, VLANs, DHCP, DDNS, and IP addresses and aliases.

About this task

Consider the following guidelines when managing IPv6 interfaces.

- The command-line interface (CLI) supports IPv6 for basic network, replication, and backup commands. CLI commands manage the IPv6 addresses. You can set and view IPv6 addresses using the DD System Manage.
- Collection, directory, and MTree replication are supported over IPv6 networks, which allows you to take advantage of the IPv6 address space. Simultaneous replication over IPv6 and IPv4 networks is also supported, as is Managed File Replication using DD Boost.
- There are some restrictions for interfaces with IPv6 addresses. For example, the minimum MTU is 1280. If you try to set the MTU lower than 1280 on an interface with an IPv6 address, an error message appears and the new MTU size is rejected. If you try to set an IPv6 address on an interface with an MTU lower than 1280, an error message appears. An IPv6 address set on a VLAN which is on a physical or virtual interface will impact that physical or virtual interface. If the MTU of the physical or virtual is given an MTU less than 1280 but it has a VLAN with an IPv6 address on it, the setting of the MTU will be rejected with an error message. In addition, if the physical or virtual interface is has an MTU less than 1280 and an associated VLAN interface is given an IPv6 address, that address is rejected because the base MTU is too small.

Procedure

1. Select **Hardware** > **Ethernet** > **Interfaces**.

   The following table describes the information on the Interfaces tab.

Table 31 Interface tab label descriptions

Item	Description
Interface	The name of each interface associated with the selected system.
Enabled	Whether the interface is enabled. • Select **Yes** to enable the interface and connect it to the network. • Select **No** to disable the interface and disconnect it from the network.
DHCP	Indicates if the interface is configured manually (`no`), by a DHCP (Dynamic Host Configuration Protocol) IPv4 server (`v4`), or by a DHCP IPv6 server (`v6`).
IP Address	IP address associated with the interface. The address used by the network to identify the interface. If the interface is configured through DHCP, an asterisk appears after this value. IPv6 SLAAC and IPv6 Linklocal IP addresses are also shown.
Netmask	Netmask associated with the interface. Uses the standard IP network mask format for IPv4 address or a prefix length for IPv6 addresses. If the interface is configured through DHCP, an asterisk appears after this value.
Link	Whether the Ethernet connection is active (Yes/No).
Address Type	On an HA system, the Address Type indicates Fixed, Floating, or Interconnect.
Additional Info	Additional settings for the interface. For example, the bonding mode.
IPMI interfaces configured	Displays Yes or No and indicates if IPMI health monitoring and power management is configured for the interface.

2. To filter the interface list by interface name, enter a value in the **Interface Name** field and click **Update**.

   Filters support wildcards, such as eth*, veth*, or eth1*

3. To filter the interface list by interface type, select a value from the Interface **Type** menu and click **Update**.

   On an HA system, there is a filter dropdown to filter by IP Address Type (Fixed, Floating, or Interconnect).

4. To return the interfaces table to the default listing, click **Reset**.
5. Select an interface in the table to populate the Interface Details area.

Table 32 Interface Details label descriptions

Item	Description
Auto-generated Addresses	Displays the automatically generated IPv6 addresses for the selected interface.

Table 32 Interface Details label descriptions (continued)

Item	Description
Auto Negotiate	When this feature displays `Enabled`, the interface automatically negotiates Speed and Duplex settings. When this feature displays `Disabled`, then Speed and Duplex values must be set manually.
Cable	Shows whether the interface is Copper or Fiber. ⓘ Note: Some interfaces must be up before the cable status is valid.
Duplex	Used in conjunction with the Speed value to set the data transfer protocol. Options are Unknown, Full, Half.
Hardware Address	The MAC address of the selected interface. For example, 00:02:b3:b0:8a:d2.
Interface Name	Name of the selected interface.
Latent Fault Detection (LFD) - HA systems only	The LFD field has a `View Configuration` link, displaying a pop-up that lists LFD addresses and interfaces.
Maximum Transfer Unit (MTU)	MTU value assigned to the interface.
Speed	Used in conjunction with the Duplex value to set the rate of data transfer. Options are Unknown, 10 Mb/s, 100 Mb/s, 1000 Mb/s, 10 Gb/s, 25 Gb/s, 100 Gb/s. ⓘ Note: Auto-negotiated interfaces must be set up before speed, duplex, and supported speed are visible.
Supported Speeds	Lists all of the speeds that the interface can use.

6. To view IPMI interface configuration and management options, click **View IPMI Interfaces**.

   This link displays the **Maintenance** > **IPMI** information.

Physical interface names

The layout of physical interface names varies on different protection systems and option cards.

The physical interface name format is `eth`*Xy*, where is the slot number for an on-board port or an option card and *y* is an alphanumeric string. For example, eth0a.

- DD2200 systems provide four on-board 1G Base-T NIC ports: ethMa (top left), ethMb (top right), ethMc (bottom left), and ethMd (bottom right).
- DD6300, DD6800, and DD9300 systems provide one on-board 1G Base-T NIC port: ethMa.
- DD9500 and DD9800 systems provide four on-board 1G Base-T NIC ports: ethMa (bottom left), ethMb (top left), ethMc (bottom right), and ethMd (top right).
- For vertical I/O module NIC interfaces, the port numbering goes from top to bottom, with eth*X*a at the top.
- For most horizontal I/O module NIC interfaces, the port numbering goes from left to right, with eth*X*a on the left.

- The horizontal I/O module slots on the left-hand side (expansion riser 1) of the DD3300, DD6900, DD9400, and DD9900 systems are inverted. The port numbering on these I/O modules in these slots goes from right to left, with eth*X*a on the right.

General interface configuration guidelines

Review the general interface configuration guidelines before configuring system interfaces.

- When supporting both backup and replication traffic, if possible, use different interfaces for each traffic type so that neither traffic type impacts the other.
- When replication traffic is expected to be less than 1 Gb/s, if possible, do not use 10 GbE interfaces for replication traffic because 10 GbE interfaces are optimized for faster traffic.
- If a service uses a non-standard port and the user wants to upgrade to DD OS 7.0, or the user wants to change a service to use a non-standard port on a DD OS 7.0 system, add a net filter function for all the clients using that service to allow the client IP addresses to use the new port.
- For systems that use IPMI, if possible, reserve interface ethMa for IPMI traffic and system management traffic (using protocols such as HTTP, Telnet, and SSH). Backup data traffic should be directed to other interfaces.

Configuring physical interfaces

You must configure at least one physical interface before the system can connect to a network.

Procedure

1. Select **Hardware** > **Ethernet** > **Interfaces**.
2. Select an interface to configure.
3. Click **Configure**.
4. In the Configure Interface dialog box, determine how the interface IP address is to be set:

   Note: On an HA system, the Configure Interface dialog box has a field for whether or not to designate the Floating IP (Yes/No). Selecting **Yes** the `Manually Configure IP Address` radio button is auto-selected; Floating IP interfaces can only be manually configured.

   - Use DHCP to assign the IP address—in the IP Settings area, select **Obtain IP Address using DHCP** and select either **DHCPv4** for IPv4 access or **DHCPv6** for IPv6 access. Setting a physical interface to use DHCP automatically enables the interface.

     Note: If you choose to obtain the network settings through DHCP, you can manually configure the hostname at **Hardware** > **Ethernet** > **Settings** or with the `net set hostname` command. You must manually configure the host name when using DHCP over IPv6.

   - Specify IP Settings manually—in the IP Settings area, select **Manually configure IP Address**.
     The **IP Address** and **Netmask** fields become active.

5. If you chose to manually enter the IP address, enter an IPv4 or IPv6 address. If you entered an IPv4 address, enter a netmask address.

   Note: You can assign just one IP address to an interface with this procedure. If you assign another IP address, the new address replaces the old address. To attach an additional IP address to an interface, create an IP alias.

6. Specify Speed/Duplex settings.

The combination of speed and duplex settings define the rate of data transfer through the interface. Select one of these options:

- **Autonegotiate Speed/Duplex** — Select this option to allow the network interface card to autonegotiate the line speed and duplex setting for an interface. Autonegotiation is *not* supported on the following DD2200, DD6300, DD6800, DD9300. DD9500, and DD9800 I/O modules:
  - Dual port 10GbE SR Optical with LC connectors (using SFPs)
  - Dual port 10GbE Direct Attach Copper (SFP+ cables)
  - Quad port 2 port 1GbE Copper (RJ45) /2 port 1GbE SR Optical
  - **Autonegotiate Speed/Duplex** is required for all I/O modules on the DD6900, DD9400, and DD9900 systems:
    - Quad port 10GbE Base-T
    - Quad port 10GbE SFP+
    - Dual port 25GbE SFP28
    - Dual port 100GbE QSFP28
- **Manually configure Speed/Duplex** — Select this option to manually set an interface data transfer rate. Select the speed and duplex from the menus.
  ⓘ | Note: This option is not available on DD6900, DD9400, and DD9900 systems.
  - Duplex options are half-duplex, full-duplex, and unknown.
  - Speed options listed are limited to the capabilities of the hardware device. Options are 10 Mb, 100 Mb, 1000 Mb (1 Gb), 10 Gb, and unknown. The 10G Base-T hardware supports only the 100 Mb, 1000 Mb and 10 Gb settings.
  - Half-duplex is only available for 10 Mb and 100 Mb speeds.
  - 1 Gb and 10 Gb line speeds require full-duplex.
  - The default setting for 10G Base-T interfaces is Autonegotiate Speed/Duplex. If you manually set the speed to 1000 Mb or 10 Gb, you must set the Duplex setting to Full.

7. Specify the MTU (Maximum Transfer Unit) size for the physical (Ethernet) interface.

   Do the following:

   - Click the **Default** button to return the setting to the default value.
   - Ensure that all of your network components support the size set with this option.

8. Optionally, select **Dynamic DNS Registration**.

   Dynamic DNS (DDNS) is a protocol that registers local IP addresses on a Domain Name System (DNS) server. In this release, DD System Manager supports Windows mode DDNS. To use UNIX mode DDNS, use the `net ddns` CLI command.

   The DDNS must be registered to enable this option.

   ⓘ | Note: This option disables DHCP for this interface.

9. Click **Next**.

   The Configure Interface Settings summary page appears. The values listed reflect the new system and interface state, which are applied after you click Finish.

10. Click **Finish** and **OK**.

MTU size values

The MTU size must be set properly to optimize the performance of a network connection. An incorrect MTU size can negatively affect interface performance.

Supported values for setting the maximum Transfer Unit (MTU) size for the physical (Ethernet) interface range from 350 to 9000 for IPv4, and 1280 to 9000 for IPv6. For 100 Base-T and gigabit networks, 1500 is the standard default.

Note: The minimum MTU for IPv6 interfaces is 1280. The interface fails if you try to set the MTU lower than 1280.

Moving a static IP address

A specific static IP address must be assigned to only one interface on a system. A static IP address must be properly removed from one interface before it is configured on another interface.

Procedure

1. If the interface that hosts the static IP address is part of a DD Boost interface group, remove the interface from that group.
2. Select **Hardware** > **Ethernet** > **Interfaces**.
3. Remove the static IP address that you want to move.
   a. Select the interface that is currently using the IP address you want to move.
   b. In the Enabled column, select **No** to disable the interface.
   c. Click **Configure**.
   d. Set the IP Address to 0.

      Note: Set the IP address to 0 when there is no other IP address to assign to the interface. The same IP address must not be assigned to multiple interfaces.

   e. Click **Next**, and click **Finish**.
4. Add the removed static IP address to another interface.
   a. Select the interface to which you want to move the IP address.
   b. In the Enabled column, select **No** to disable the interface.
   c. Click **Configure**.
   d. Set the IP Address to the match the static IP address you removed.
   e. Click **Next**, and click **Finish**.
   f. In the Enabled column, select **Yes** to enable the updated interface.

Virtual interface configuration guidelines

Virtual interface configuration guidelines apply to failover and aggregate virtual interfaces. There are additional guidelines that apply to either failover or aggregate interfaces but not both.

- The *virtual-name* must be in the form `vethx` where *x* is a number. The recommended maximum number is 99 because of name size limitations.
- You can create as many virtual interfaces as there are physical interfaces.
- Each interface used in a virtual interface must first be disabled. An interface that is part of a virtual interface is seen as disabled for other network configuration options.
- After a virtual interface is destroyed, the physical interfaces associated with it remain disabled. You must manually re-enable the physical interfaces.

- The number and type of cards installed determines the number of Ethernet ports available.
- Each physical interface can belong to one virtual interface.
- A system can support multiple mixed failover and aggregation virtual interfaces, subject to the restrictions above.
- Virtual interfaces must be created from identical physical interfaces. For example, all copper, all optical, all 1 Gb, or all 10 Gb. However, 1 Gb interfaces support bonding a mix of copper and optical interfaces. This applies to virtual interfaces across different cards with identical physical interfaces, except for Chelsio cards. For Chelsio cards, only failover is supported, and that is only across interfaces on the same card.
- Failover and aggregate links improve network performance and resiliency by using two or more network interfaces in parallel, thus increasing the link speed for aggregated links and reliability over that of a single interface.
- Remove functionality is available using the **Configure** button. Click a virtual interface in the list of interfaces on the Interfaces tab and click **Configure**. From the list of interfaces in the dialog box, clear the checkbox for the interface to remove it from bonding (failover or aggregate), and click **Next**.
- For a bonded interface, the bonded interface is created with remaining slaves if the hardware for a slave interface fails. If no slaves, the bonded interface id created with no slaves. This slave hardware failure will generate managed alerts, one per failed slave.

  Note: The alert for a failed slave disappears after the failed slave is removed from the system. If new hardware is installed, the alerts disappear and the bonded interface uses the new slave interface after the reboot.
- On DD3300 systems, the ethMa interface does not support failover or link aggregation.

Guidelines for configuring a virtual interface for link aggregation

Link aggregation provides improved network performance and resiliency by using one or more network interfaces in parallel, thus increasing the link speed and reliability over that of a single interface. These guidelines are provided to help you optimize your use of link aggregation.

- Changes to disabled Ethernet interfaces flush the routing table. It is recommended that you make interface changes only during scheduled maintenance downtime. Afterwards, re-configure the routing rules and gateways.
- Enable aggregation on an existing virtual interface by specifying the physical interfaces and mode and giving it an IP address.
- 10 Gb single-port optical Ethernet cards do not support link aggregation.
- 1 GbE and 10 GbE interfaces cannot be aggregated together.
- Copper and optical interfaces cannot be aggregated together.

Guidelines for configuring a virtual interface for failover

Link failover provides improved network stability and performance by identifying backup interfaces that can support network traffic when the primary interface is not operating. These guidelines are provided to help you optimize your use of link failover.

- A primary interface must be part of the failover. If a primary interface removal is attempted from a failover, an error message appears.
- When a primary interface is used in a failover configuration, it must be explicitly specified and must also be a bonded interface to the virtual interface. If the primary interface goes down and multiple interfaces are still available, the next interface is randomly selected.

- All interfaces in a virtual interface must be on the same physical network. Network switches used by a virtual interface must be on the same physical network.
- The recommended number of physical interfaces for failover is greater than one. You can, however, configure one primary interface and one or more failover interfaces, except with 10 Gb CX4 Ethernet cards, which are restricted to one primary interface and one failover interface from the same card

Virtual interface creation

Create a virtual interface to support link aggregation or failover. The virtual interface serves as a container for the links to be aggregated or associated for failover.

Creating a virtual interface for link aggregation

Create a virtual interface for link aggregation to serve as a container to associate the links that participate in aggregation.

About this task

A link aggregation interface must specify a link bonding mode and may require a hash selection. For example, you might enable link aggregation on virtual interface *veth1* to physical interfaces *eth1* and *eth2* in mode LACP (Link Aggregation Control Protocol) and hash XOR-L2L3.

Procedure

1. Select **Hardware** > **Ethernet** > **Interfaces**.
2. In the Interfaces table, disable the physical interface where the virtual interface is to be added by clicking **No** in the **Enabled** column.
3. From the **Create** menu, select **Virtual Interface**.
4. In the Create Virtual Interface dialog box, specify a virtual interface name in the **veth** box.

   Enter a virtual interface name in the form *vethx*, where *x* is a unique ID (typically one or two digits). A typical full virtual interface name with VLAN and IP Alias is *veth56.3999:199*. The maximum length of the full name is 15 characters. Special characters are not allowed. Numbers must be between 0 and 4094, inclusively.

5. In the **Bonding Type** list, select **Aggregate**.

   Note: Registry settings can be different from the bonding configuration. When interfaces are added to the virtual interface, the information is not sent to the bonding module until the virtual interface is given an IP address and brought up. Until that time the registry and the bonding driver configuration are different.

6. In the **Mode** list, select a bonding mode.

   Specify the mode that is compatible with the requirements of the system to which the interfaces are directly attached.

   - Round-robin
     Transmit packets in sequential order from the first available link through the last in the aggregated group.
   - Balanced
     Data is sent over interfaces as determined by the hash method selected. This requires the associated interfaces on the switch to be grouped into an Ether channel (trunk) and given a hash via the Load Balance parameter.
   - LACP
     Link Aggregation Control Protocol is similar to Balanced, except that it uses a control protocol that communicates to the other end and coordinates which links within the

bond are available for use. LACP provides a kind of heartbeat failover and must be configured at both ends of the link.

7. If you selected Balanced or LACP mode, specify a bonding hash type in the **Hash** list.

   Options are: XOR-L2, XOR-L2L3, or XOR-L3L4.

   XOR-L2 transmits through a bonded interface with an XOR hash of Layer 2 (inbound and outbound MAC addresses).

   XOR-L2L3 transmits through a bonded interface with an XOR hash of Layer 2 (inbound and outbound MAC addresses) and Layer 3 (inbound and outbound IP addresses).

   XOR-L3L4 transmits through a bonded interface with an XOR hash of Layer 3 (inbound and outbound IP addresses) and Layer 4 (inbound and outbound ports).

8. To select an interface to add to the aggregate configuration, select the checkbox that corresponds to the interface, and then click **Next**.

   The Create virtual interface *veth_name* dialog box appears.

9. Enter an IP address, or enter `0` to specify no IP address.
10. Enter a netmask address or prefix.
11. Specify Speed/Duplex options.

    The combination of speed and duplex settings define the rate of data transfer through the interface. Select either:

    - **Autonegotiate Speed/Duplex**
      Select this option to allow the network interface card to autonegotiate the line speed and duplex setting for an interface.
    - **Manually configure Speed/Duplex**
      Select this option to manually set an interface data transfer rate.
      - Duplex options are half-duplex or full-duplex.
      - Speed options listed are limited to the capabilities of the hardware device. Options are 10 Mb, 100 Mb, 1000 Mb, and 10 Gb.
      - Half-duplex is only available for 10 Mb and 100 Mb speeds.
      - 1000 Mb and 10 Gb line speeds require full-duplex.
      - Optical interfaces require the Autonegotiate option.
      - The 10 GbE copper NIC default is 10 Gb. If a copper interface is set to 1000 Mb or 10 Gb line speed, duplex must be full-duplex.

12. Specify the MTU setting.
    - To select the default value (1500), click **Default**.
    - To select a different setting, enter the setting in the **MTU** box. Ensure that all of your network components support the size set with this option.

13. Optionally, select Dynamic DNS Registration option.

    Dynamic DNS (DDNS) is a protocol that registers local IP addresses on a Domain Name System (DNS) server. In this release, DD System Manager supports Windows mode DDNS. To use UNIX mode DDNS, use the `net ddns` CLI command.

    The DDNS must be registered to enable this option.

14. Click **Next**.

The Configure Interface Settings summary page appears. The values listed reflect the new system and interface state.

15. Click **Finish** and **OK**.

Creating a virtual interface for link failover

Create a virtual interface for link failover to serve as a container to associate the links that will participate in failover.

About this task

The failover-enabled virtual interface represents a group of secondary interfaces, one of which can be specified as the primary. The system makes the primary interface the active interface whenever the primary interface is operational. A configurable Down Delay failover option allows you to configure a failover delay in 900 millisecond intervals. The failover delay guards against multiple failovers when a network is unstable.

Procedure

1. Select **Hardware** > **Ethernet** > **Interfaces**.
2. In the interfaces table, disable the physical interface to which the virtual interface is to be added by clicking **No** in the **Enabled** column.
3. From the **Create** menu, select **Virtual Interface**.
4. In the Create Virtual Interface dialog box, specify a virtual interface name in the **veth** box.

   Enter a virtual interface name in the form `vethx`, where *x* is a unique ID (typically one or two digits). A typical full virtual interface name with VLAN and IP Alias is *veth56.3999:199*. The maximum length of the full name is 15 characters. Special characters are not allowed. Numbers must be between 0 and 4094, inclusively.

5. In the **Bonding Type** list, select **Failover**.
6. Select an interface to add to the failover configuration, and click **Next**. Virtual aggregate interfaces can be used for failover.

   The Create virtual interface *veth_name* dialog box appears.

7. Enter an IP address, or enter `0` to specify no IP address.
8. Enter a netmask or prefix.
9. Specify the Speed/Duplex options.

   The combination of speed and duplex settings defines the rate of data transfer through the interface.

   - Select **Autonegotiate Speed/Duplex** to allow the network interface card to autonegotiate the line speed and duplex setting for an interface.
   - Select **Manually configure Speed/Duplex** to manually set an interface data-transfer rate.

     Note: This option is not available on DD6900, DD9400, and DD9900 systems.

     - Duplex options are either half duplex or full duplex.
     - Speed options listed are limited to the capabilities of the hardware device. Options are 10 Mb, 100 Mb, 1000 Mb, and 10 Gb.
     - Half-duplex is available for 10 Mb and 100 Mb speeds only.
     - 1000 Mb and 10 Gb line speeds require full-duplex.
     - Optical interfaces require the Autonegotiate option.

- The copper interface default is 10 Gb. If a copper interface is set to 1000 Gb or 10 Gb line speed, the duplex must be full-duplex.

10. Specify MTU setting.
    - To select the default value (1500), click **Default**.
    - To select a different setting, enter the setting in the MTU box. Ensure that all of your network path components support the size set with this option.
11. Optionally, select Dynamic DNS Registration option.

    Dynamic DNS (DDNS) is a protocol that registers local IP addresses on a Domain Name System (DNS) server. In this release, DD System Manager supports Windows mode DDNS. To use UNIX mode DDNS, use the `net ddns` CLI command.

    The DDNS must be registered to enable this option.

    Note: This option disables DHCP for this interface.
12. Click **Next**.

    The Configure Interface Settings summary page appears. The values listed reflect the new system and interface state.
13. Complete the Interface, click **Finish** and **OK**.

Modifying a virtual interface

After you create a virtual interface, you can update the settings to respond to network changes or resolve issues.

Procedure

1. Select **Hardware** > **Ethernet** > **Interfaces**.
2. In the Interfaces column, select the interface and disable the virtual interface by clicking **No** in the **Enabled** column. Click **OK** in the warning dialog box.
3. In the **Interfaces** column, select the interface and click **Configure**.
4. In the **Configure Virtual Interface** dialog box, change the settings.
5. Click **Next** and **Finish**.

Configuring a VLAN

Create a new VLAN interface from either a physical interface or a virtual interface.

About this task

The recommended total VLAN count is 80. You can create up to 100 interfaces (minus the number of aliases, physical and virtual interfaces) before the system prevents you from creating any more.

Procedure

1. Select **Hardware** > **Ethernet** > **Interfaces**.
2. In the interfaces table, select the interface to which you want to add the VLAN.
3. Click **Create** and select**VLAN**.
4. In the Create VLAN dialog box, specify a VLAN ID by entering a number in the **VLAN Id** box.

   The range of a VLAN ID is between 1 and 4094 inclusive.

5. Enter an IP address, or enter 0 to specify no IP address.

   The Internet Protocol (IP) address is the numerical label assigned to the interface. For example, 192.168.10.23.

6. Enter a netmask or prefix.
7. Specify the MTU setting.

   The VLAN MTU must be less than or equal to the MTU defined for the physical or virtual interface to which it is assigned. If the MTU defined for the supporting physical or virtual interface is reduced below the configured VLAN value, the VLAN value is automatically reduced to match the supporting interface. If the MTU value for the supporting interface is increased above the configured VLAN value, the VLAN value is unchanged.

   - To select the default value (1500), click **Default**.
   - To select a different setting, enter the setting in the MTU box. DD System Manager does not accept an MTU size that is larger than that defined for the physical or virtual interface to which the VLAN is assigned.

8. Specify Dynamic DNS Registration option.

   Dynamic DNS (DDNS) is a protocol that registers local IP addresses on a Domain Name System (DNS) server. In this release, DD System Manager supports Windows mode DDNS. To use UNIX mode DDNS, use the `net ddns` CLI command.

   The DDNS must be registered to enable this option.

9. Click **Next.**

   The **Create VLAN** summary page appears.

10. Review the configuration settings, click **Finish**, and click **OK.**

Modifying a VLAN interface

After you create a VLAN interface, you can update the settings to respond to network changes or resolve issues.

Procedure

1. Select **Hardware** > **Ethernet** > **Interfaces**.
2. In the **Interfaces** column, select the checkbox of the interface and disable the VLAN interface by clicking **No** in the **Enabled** column. Click **OK** in the warning dialog box.
3. In the Interfaces column, select the checkbox of the interface and click **Configure**.
4. In the **Configure VLAN Interface** dialog box, change the settings.
5. Click **Next** and **Finish**.

Configuring an IP alias

An IP alias assigns an additional IP address to a physical interface, a virtual interface, or a VLAN.

About this task

The recommended total number of IP aliases, VLAN, physical, and virtual interfaces that can exist on the system is 80. Although up to 100 interfaces are supported, as the maximum number is approached, you might notice slowness in the display.

ⓘ Note: When using an HA pair, aliases cannot be created on the standby node. Create the alias on the active node then configure it on the standby node.

Procedure

1. Select **Hardware** > **Ethernet** > **Interfaces**.
2. Click **Create**, and select **IP Alias**.

   The Create IP Alias dialog box appears.
3. Specify an IP alias ID by entering a number in the **IP ALIAS Id** box.

   The range is 1 to 4094 inclusive.
4. Enter an IPv4 or IPv6 address.
5. If you entered an IPv4 address, enter a netmask address.
6. Specify Dynamic DNS Registration option.

   Dynamic DNS (DDNS) is a protocol that registers local IP addresses on a Domain Name System (DNS) server. In this release, DD System Manager supports Windows mode DDNS. To use UNIX mode DDNS, use the `net ddns` CLI command.

   The DDNS must be registered to enable this option.
7. Click **Next**.

   The Create IP Alias summary page appears.
8. Review the configuration settings, click **Finish**, and **OK**.

Modifying an IP alias interface

After you create an IP alias, you can update the settings to respond to network changes or resolve issues.

Procedure

1. Select **Hardware** > **Ethernet** > **Interfaces**.
2. In the **Interfaces** column, select the checkbox of the interface and disable the IP alias interface by clicking **No** in the **Enabled** column. Click **OK** in the warning dialog box.
3. In the **Interfaces** column, select the checkbox of the interface and click **Configure**.
4. In the Configure IP Alias dialog box, change the settings as described in the procedure for creating an IP Alias.
5. Click **Next** and **Finish**.

Registering interfaces with DDNS

Dynamic DNS (DDNS) is a protocol that registers local IP addresses on a Domain Name System (DNS) server.

About this task

In this release, DD System Manager supports Windows mode DDNS. To use UNIX mode DDNS, use the `net ddns` CLI command. You can do the following.

- Manually register (add) configured interfaces to the DDNS registration list.
- Remove interfaces from the DDNS registration list.
- Enable or disable DNS updates.
- Display whether DDNS registration is enabled or not.
- Display interfaces in the DDNS registration list.

Procedure

1. Select **Hardware** > **Ethernet** > **Interfaces** > **DDNS Registration**.
2. In the DDNS Windows Mode Registration dialog box, click **Add** to add an interface to the DDNS.

   The Add Interface dialog box appears.

   a. Enter a name in the **Interface** field.

   b. Click **OK**.
3. Optionally, to remove an interface from the DDNS:

   a. Select the interface to remove, and click **Remove**.

   b. In the Confirm Remove dialog box, click **OK**.
4. Specify the DDNS Status.
   - Select **Enable** to enable updates for all interfaces already registered.
   - Click **Default** to select the default settings for DDNS updates.
   - Clear **Enable** to disable DDNS updates for the registered interfaces.
5. To complete the DDNS registration, click **OK**.

Destroying an interface

You can use DD System Manager to destroy or delete virtual, VLAN, and IP alias interfaces.

About this task

When a virtual interface is destroyed, the system deletes the virtual interface, releases its bonded physical interface, and deletes any VLANs or aliases attached to the virtual interface. When you delete a VLAN interface, the OS deletes the VLAN and any IP alias interfaces that are created under it. When you destroy an IP alias, the OS deletes only that alias interface.

Procedure

1. Select **Hardware** > **Ethernet** > **Interfaces**.
2. Click the box next to each interface you want to destroy (Virtual or VLAN or IP Alias).
3. Click **Destroy**.
4. Click **OK** to confirm.

Viewing an interface hierarchy in the tree view

The Tree View dialog box displays the association between physical and virtual interfaces.

Procedure

1. Select **Hardware** > **Ethernet** > **Interfaces** > **Tree View**.
2. In the Tree View dialog box, click the plus or minus boxes to expand or contract the tree view that shows the hierarchy.
3. Click **Close** to exit this view.

General network settings management

The configuration settings for hostname, domain name, search domains, host mapping, and DNS list are managed together on the Settings tab.

Viewing network settings information

The Settings tab displays the current configuration for the hostname, domain name, search domains, host mapping, and DNS.

Procedure

1. Select **Hardware** > **Ethernet** > **Settings**.

Results

The Settings tab displays the following information.

Host Settings

Host Name

The hostname of the selected system.

Domain Name

The fully qualified domain name associated with the selected system.

Search Domain List

Search Domain

A list of search domains that the selected system uses. The system applies the search domain as a suffix to the hostname.

Hosts Mapping

IP Address

IP address of the host to resolve.

Host Name

Hostnames associated with the IP address.

DNS List

DNS IP Address

Current DNS IP addresses associated with the selected system. An asterisk (*) indicates that the IP addresses were assigned through DHCP.

Setting the DD System Manager hostname

You can configure the DD System Manager hostname and domain name manually, or you can configure DD OS to automatically receive the host and domain names from a Dynamic Host Configuration Protocol (DHCP) server.

About this task

One advantage to manually configuring the host and domain names is that you remove the dependency on the DHCP server and the interface leading to the DHCP server. To minimize the risk of service interruption, if possible, manually configure the host and domain names.

When configuring the hostname and domain name, consider the following guidelines.

- Do not include an underscore in the hostname; it is incompatible with some browsers.
- Replication and CIFS authentication must be reconfigured after you change the names.

- If a system was previously added without a fully qualified name (no domain name), a domain name change requires that you remove and add the affected system or update the Search Domain List to include the new domain name.

Note: For steps on changing an established hostname, see KB article 182164.

Procedure

1. Select **Hardware** > **Ethernet** > **Settings**.
2. Click **Edit** in the **Host Settings** area. The **Configure Host** dialog opens.
3. To manually configure the host and domain names:
   a. Select **Manually configure host**.
   b. Enter a hostname in the **Host Name** box.
      For example, `id##.yourcompany.com`
   c. Enter a domain name in the **Domain Name** box.
      This is the domain name that is associated with your protection system and, usually, your company's domain name. For example, *yourcompany.com*
   d. Click **OK**.
      The system displays progress messages as the changes are applied.
4. To obtain the host and domain names from a DHCP server, select **Obtain Settings using DHCP** and click **OK**.
   At least one interface must be configured to use DHCP.

Managing the domain search list

Use the domain search list to define which domains the system can search.

Procedure

1. Select **Hardware** > **Ethernet** > **Settings**.
2. Click **Edit** in the Search Domain List area.
3. To add a search domain using the Configure Search Domains dialog:
   a. Click Add (+).
   b. In the Add Search Domain dialog, enter a name in the **Search Domain** box.
      For example, `id##.yourcompany.com`
   c. Click **OK**.
      The system adds the new domain to the list of searchable domains.
   d. Click **OK** to apply changes and return to the Settings view.
4. To remove a search domain using the Configure Search Domains dialog:
   a. Select the search domain to remove.
   b. Click Delete (**X**).
      The system removes the selected domain from the list of searchable domains.
   c. Click **OK** to apply changes and return to the Settings view.

Adding and deleting host maps

A host map links an IP address to a hostname, so that either the IP address or the hostname can be used to specify the host.

Procedure

1. Select **Hardware** > **Ethernet** > **Settings**.
2. To add a host map, do the following.
   a. In the Hosts Mapping area, click **Add**.
   b. In the Add Hosts dialog, enter the IP address of the host in the **IP Address** box.
   c. Click Add (+).
   d. In the Add Host dialog, enter a hostname, such as `id##.yourcompany.com`, in the **Host Name** box.
   e. Click **OK** to add the new hostname to the Host Name list.
   f. Click **OK** to return to the Settings tab.
3. To delete a host map, do the following.
   a. In the Hosts Mapping area, select the host mapping to delete.
   b. Click Delete (**X**).

Configuring DNS IP addresses

DNS IP addresses specify the DNS servers the system can use to get IP addresses for host names that are not in the host mapping table.

About this task

You can configure the DNS IP addresses manually, or you can configure DD OS to automatically receive IP addresses from a DHCP server. One advantage to manually configuring DNS IP addresses is that you remove the dependency on the DHCP server and the interface leading to the DHCP server. To minimize the risk of service interruption, EMC recommends that you manually configure the DNS IP addresses.

Procedure

1. Select **Hardware** > **Ethernet** > **Settings**.
2. Click **Edit** in the DNS List area.
3. To manually add a DNS IP address:
   a. Select **Manually configure DNS list**.
      The DNS IP address checkboxes become active.
   b. Click Add (+).
   c. In the Add DNS dialog box, enter the DNS IP address to add.
   d. Click **OK**.
      The system adds the new IP address to the list of DNS IP addresses.
   e. Click **OK** to apply the changes.
4. To delete a DNS IP address from the list:
   a. Select **Manually configure DNS list**.
      The DNS IP address checkboxes become active.

b. Select the DNS IP address to delete and click Delete (**X**).

The system removes the IP address from the list of DNS IP addresses.

c. Click **OK** to apply the changes.

5. To obtain DNS addresses from a DHCP server, select **Obtain DNS using DHCP** and click **OK**.

At least one interface must be configured to use DHCP.

Network route management

Routes determine the path taken to transfer data to and from the localhost (the protection system) to another network or host.

Data Domain and PowerProtect systems do not generate or respond to any of the network routing management protocols (RIP, EGRP/EIGRP, and BGP). The only routing implemented on a protection system is IPv4 policy-based routing, which allows only one route to a default gateway per routing table. There can be multiple routing tables and multiple default gateways. A routing table is created for each address that has the same subnet as a default gateway. The routing rules send the packets with the source IP address that matches the IP address used to create the table to that routing table. All other packets that do not have source IP addresses that match a routing table are sent to the main routing table.

Within each routing table, static routes can be added, but because source routing is used to get packets to the table, the only static routes that will work are static routes that use the interface that has the source address of each table. Otherwise it needs to be put into the main table.

Static routes are also required in the main routing table to direct which source addresses to use with connections initiated from DD OS if the destination program does not bind the IP address.

ⓘ Note: DD Replicator sets a static route between the source and target systems when the replication context is created, therefore it does not require the creation of additional static routes.

Other than the IPv4 source routing done to these other routing tables, Data Domain and PowerProtect systems use source-based routing for the main routing IPv4 and IPv6 tables, which means that outbound network packets that match the subnet of multiple interfaces are routed only over the physical interface whose IP address matches the source IP address of the packets, which is where they originated.

For IPv6, set static routes when multiple interfaces contain the same IPv6 subnets, and the connections are being made to IPv6 addresses with this subnet. Normally, static routes are not needed with IPv4 addresses with the same subnet, such as for backups. There are cases in which static addresses may be required to allow connections to work, such as connections from the protection system to remote systems.

Static routes can be added and deleted from individual routing tables by adding or deleting the table from the route specification. This provides the rules to direct packets with specific source addresses through specific route tables. If a static route is required for packets with those source addresses, the routes must be added the specific table where the IP address is routed.

ⓘ Note: Routing for connections initiated from the protection system, such as for replication, depends on the source address used for interfaces on the same subnet. To force traffic for a specific interface to a specific destination (even if that interface is on the same subnet as other interfaces), configure a static routing entry between the two systems: this static routing overrides source routing. This is not needed if the source address is IPv4 and has a default gateway associated with it. In that case, the source routing is already handled via its own routing table.

Viewing route information

The Routes tab displays the default gateways, static routes, and dynamic routes.

Procedure

1. Select **Hardware** > **Ethernet** > **Routes**.

   Note: If this does not display all the routing tables configured on the system, run the `net route show tables` command to display all the tables. The *DD OS Command Reference Guide* provides additional information.

Results

The Static Routes area lists the route specification used to configure each static route. The Dynamic Routes table lists information for each of the dynamically assigned routes.

Table 33 Dynamic Routes column label descriptions

Item	Description
Destination	The destination host/network where the network traffic (data) is sent.
Gateway	The address of the router in the DD network, or 0.0.0.0 if no gateway is set.
Genmask	The netmask for the destination net. Set to 255.255.255.255 for a host destination and 0.0.0.0 for the default route.
Flags	Possible flags include: U—Route is up, H—Target is a host, G —Use gateway, R —Reinstate route for dynamic routing, D—Dynamically installed by daemon or redirect, M —Modified from routing daemon or redirect, A —Installed by addrconf, C —Cache entry, and ! —Reject route.
Metric	The distance to the target (usually counted in hops). Not used by the DD OS, but might be needed by routing daemons.
MTU	Maximum Transfer Unit (MTU) size for the physical (Ethernet) interface.
Window	Default window size for TCP connections over this route.
IRTT	Initial RTT (Round Trip Time) used by the kernel to estimate the best TCP protocol parameters without waiting on possibly slow answers.
Interface	Interface name associated with the routing interface.

Setting the default gateway

You can configure the default gateway manually, or you can configure DD OS to automatically receive the default gateway IP addresses from a DHCP server.

About this task

One advantage to manually configuring the default gateway is that you remove the dependency on the DHCP server and the interface leading to the DHCP server. To minimize the risk of service interruption, if possible, manually configure the default gateway IP address.

Note: The system supports the use of additional default gateways that are configured on specific NICs. Use the `net route add gateway` command to configure additional default gateways. The *DD OS Command Reference Guide* provides additional information.

Procedure

1. Select **Hardware** > **Ethernet** > **Routes**.
2. Click **Edit** next to the default gateway type (IPv4 or IPv6) you want to configure.
3. To manually configure the default gateway address:
   a. Select **Manually Configure**.
   b. Enter the gateway address in the **Gateway** box.
   c. Click **OK**.
4. To obtain the default gateway address from a DHCP server, select **Use DHCP value** and click **OK**.

   At least one interface must be configured to use DHCP.

Creating static routes

Static routes define destination hosts or networks that they system can communicate with.

About this task

Note: The steps for adding a static route using the CLI can be found in KB article 500223.

Procedure

1. Select **Hardware** > **Ethernet** > **Routes**.
2. Click **Create** in the Static Routes area.
3. In the **Create Routes** dialog, select the interface you want to host the static route, and click **Next**.
4. Specify the Destination.
   - To specify a destination network, select **Network** and enter the network address and netmask for the destination network.
   - To specify a destination host, select **Host** and enter the hostname or IP address of the destination host.
5. Optionally, specify the gateway to use to connect to the destination network or host.
   a. Select **Specify a gateway for this route**.
   b. Enter the gateway address in the **Gateway** box.
6. Review the configuration and click **Next**.

   The create routes Summary page appears.
7. Click **Finish**.
8. After the process is completed, click **OK**.

   The new route specification is listed in the Route Spec list.

Deleting static routes

Delete a static route when you no longer want the system to communicate with a destination host or network.

Procedure

1. Select **Hardware** > **Ethernet** > **Routes**.
2. Select the Route Spec of the route specification to delete.

3. Click **Delete**.
4. Click **Delete** to confirm and then click **Close**.

   The selected route specification is removed from the Route Spec list.

System passphrase management

The system passphrase is a key that allows a protection system to be transported with encryption keys on the system. The encryption keys protect the data and the system passphrase protects the encryption keys.

The system passphrase is a human-readable (understandable) key (like a password) which is used to generate a machine usable AES 256 encryption key. If the system is stolen in transit, an attacker cannot easily recover the data; at most, they can recover the encrypted user data and the encrypted keys.

The passphrase is stored internally on a hidden part the storage subsystem. This allows the protection system to boot and continue servicing data access without any administrator intervention.

Setting the system passphrase

The system passphrase must be set before the system can support data encryption or request digital certificates.

Before you begin

No minimum system passphrase length is configured when DD OS is installed, but the CLI provides a command to set a minimum length. To determine if a minimum length is configured for the passphrase, enter the `system passphrase option show` CLI command.

Procedure

1. Select **Administration** > **Access** > **Administrator Access**.

   If the system passphrase is not set, the **Set Passphrase** button appears in the Passphrase area. If a system passphrase is configured, the **Change Passphrase** button appears, and your only option is to change the passphrase.

2. Click the **Set Passphrase** button.

   The Set Passphrase dialog appears.

3. Enter the system passphrase in the boxes and click **Next**.

   If a minimum length is configured for the system passphrase, the passphrase you enter must contain the minimum number of characters.

Results

The system passphrase is set and the **Change Passphrase** button replaces the **Set Passphrase** button.

Changing the system passphrase

The administrator can change the passphrase without having to manipulate the actual encryption keys. Changing the passphrase indirectly changes the encryption of the keys, but does not affect user data or the underlying encryption key.

About this task

⚠ WARNING Be sure to take care of the passphrase. If the passphrase is lost, you can never unlock the file system and access the data; the data is irrevocably lost.

Changing the passphrase requires two-user authentication to protect against data shredding.

Procedure

1. Select **Administration** > **Access** > **Administrator Access**.
2. To change the system passphrase, click **Change Passphrase**.

   The Change Passphrase dialog appears.

   ⓘ Note: The file system must be disabled to change the passphrase. If the file system is running, you are prompted to disable it.

3. In the text fields, provide:
   - The user name and password of a Security Officer account (an authorized user in the Security User group on that system).
   - The current passphrase when changing the passphrase.
   - The new passphrase, which must contain the minimum number of characters configured with the `system passphrase option set min-length` command.
4. Click the checkbox for **Enable file system now**.
5. Click **OK**.

Configuring mail server settings

The Mail Server tab allows you to specify the mail server to which DD OS sends email reports.

About this task

Procedure

1. Select **Administration** > **Settings** > **Mail Server**.
2. Select **More Tasks** > **Set Mail Server**.

   The Set Mail Server dialog box appears.

3. Specify the name of the mail server in the **Mail Server** field.
4. Use the **Credentials** button to enable or disable the use of credentials for the mail server.
5. If credentials are enabled, specify the mail server username in the **User Name** field.
6. If credentials are enabled, specify the mail server password in the **Password** field.
7. Click **Set**.
8. Optionally use the CLI to verify and troubleshoot the mail server configuration.
   a. Run the `config show mailserver` command to verify the mail server is configured.

b. Run the `net ping <mailserver-hostname> count 4` command to ping the mail server.

c. If the mail server is not configured correctly, run the `config set mailserver <mailserver-hostname>` command to set the mail server, and attempt to ping it again.

d. Run the `net show dns` command to verify the DNS server is configured.

e. Run the `net ping <DNS-hostname> count 4` command to ping the DNS server.

f. If the DNS server is not configured correctly, run the `config set dns <dns-IP>` command to set the DNS server, and attempt to ping it again.

g. Optionally run the `net hosts add <IP-address> <hostname>` command to add the mail server IP address and hostname to the system hosts file for local resolving.

h. Run the `net ping <mailserver-hostname> count 4` command to ping the mail server.

Managing system properties

The System Properties tab enables you to view and configure system properties that identify the managed system location, administrator email address, and host name.

Procedure

1. To view the current configuration, select **Administration** > **Settings** > **System Properties**.

   The System Properties tab displays the system location, the administrator email address, and the administrator hostname.

2. To change the configuration, select **More Tasks** > **Set System Properties**.

   The Set System Properties dialog box appears.

3. In the **Location** box, enter information about where the protection system is located.
4. In the **Admin Email** box, enter the email address of the system administrator.
5. In the **Admin Host** box, enter the name of the administration server.
6. Click **OK**.

SNMP management

The Simple Network Management Protocol (SNMP) is a standard protocol for exchanging network management information, and is a part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP provides a tool for network administrators to manage and monitor network-attached devices, such as protection systems, for conditions that warrant administrator attention.

To monitor systems using SNMP, you will need to install the DD OS MIB in your SNMP Management system. DD OS also supports the standard MIB-II so you can also query MIB-II statistics for general data such as network statistics. For full coverage of available data you should utilize both the DD OS MIB and the standard MIB-II MIB.

The DD OS system SNMP agent accepts queries for system-specific information from management systems using SNMP v1, v2c, and v3. SNMP V3 provides a greater degree of security than v2c and v1 by replacing cleartext community strings (used for authentication) with user-based authentication using either MD5 or SHA1. Also, SNMP v3 user authentication packets can be encrypted and their integrity verified with either DES or AES.

Protection systems can send SNMP traps (which are alert messages) using SNMP v2c and SNMP v3. Because SNMP v1 traps are not supported, if possible, use SNMP v2c or v3.

The default port that is open when SNMP is enabled is port 161. Traps are sent out through port 162.

The *DD OS MIB Quick Reference* describes the full set of MIB parameters included in the DD OS MIB branch.

Viewing SNMP status and configuration

The SNMP tab displays the current SNMP status and configuration.

Procedure

1. Select **Administration** > **Settings** > **SNMP**.

   The SNMP view shows the SNMP status, SNMP properties, SNMP V3 configuration, and SNMP V2C configuration.

SNMP tab labels

The SNMP tab labels identify the overall SNMP status, SNMP property values, and the configurations for SNMPv3 and SNMPv2.

Status

The Status area displays the operational status of the SNMP agent on the system, which is either Enabled or Disabled.

SNMP Properties

Table 34 SNMP Properties descriptions

Item	Description
SNMP System Location	The location of the protection system being monitored.
SNMP System Contact	The person designated as the contact person for system administration.
SNMP System Notes	(Optional) Additional SNMP configuration data.
SNMP Engine ID	A unique hexadecimal identifier for the system.

SNMP V3 Configuration

Table 35 SNMP Users column descriptions

Item	Description
Name	The name of the user on the SNMP manager with access to the agent for the protection system.
Access	The access permissions for the SNMP user, which can be Read-only or Read-write.
Authentication Protocols	The Authentication Protocol used to validate the SNMP user, which can be MD5, SHA1, or None.
Privacy Protocol	The encryption protocol used during the SNMP user authentication, which can be AES, DES, or None.

Table 36 Trap Hosts column descriptions

Item	Description
Host	The IP address or domain name of the SNMP management host.
Port	The port used for SNMP trap communication with the host. For example, 162 is the default.
User	The user on the trap host authenticated to access the protection SNMP information.

SNMP V2C Configuration

Table 37 Communities column descriptions

Item	Description
Community	The name of the community. For example, public, private, or localCommunity.
Access	The access permission assigned, which can be Read-only or Read-write.
Hosts	The hosts in this community.

Table 38 Trap Hosts column descriptions

Item	Description
Host	The systems designated to receive SNMP traps generated by the protection system. If this parameter is set, systems receive alert messages, even if the SNMP agent is disabled.
Port	The port used for SNMP trap communication with the host. For example, 162 is the default.
Community	The name of the community. For example, public, private, or localCommunity.

Enabling and disabling SNMP

Use the SNMP tab to enable of disable SNMP.

Procedure

1. Select **Administration** > **Settings** > **SNMP**.
2. In the Status area, click **Enable** or **Disable**.

Downloading the SNMP MIB

Use the SNMP tab to download the SNMP MIB.

Procedure

1. Select **Administration** > **Settings** > **SNMP**.
2. Click **Download MIB file**.
3. In the Opening *<protection system>*.mib dialog box, select **Open**.

4. Click **Browse** and select a browser to view the MIB in a browser window.

   Note: If using the Microsoft Internet Explorer browser, enable Automatic prompting for file download.

5. Save the MIB or exit the browser.

Configuring SNMP properties

Use the SNMP tab to configure the text entries for system location and system contact.

Procedure

1. Select **Administration** > **Settings** > **SNMP**.
2. In the SNMP Properties area, click **Configure**.

   The SNMP Configuration dialog box appears.

3. In the text fields, specify the following information: and/or an
   - SNMP System Location: A description of where the protection system is located.
   - SNMP System Contact: The email address of the system administrator.
   - SNMP System Notes: (Optional) Additional SNMP configuration information.
   - SNMP Engine ID: A unique identifier for the SNMP entity. The engine ID must be 5-34 hexadecimal characters (SNMPv3 only).

     Note: The system displays an error if the SNMP engine ID does not meet the length requirements, or uses invalid characters.

4. Click **OK**.

SNMP V3 user management

Use the SNMP tab to create, modify, and delete SNMPv3 users and trap hosts.

Creating SNMP V3 users

When you create SNMPv3 users, you define a username, specify either read-only or read-write access, and select an authentication protocol.

Procedure

1. Select **Administration** > **Settings** > **SNMP**.
2. In the SNMP Users area, click **Create**.

   The Create SNMP User dialog box appears.

3. In the **Name** text field, enter the name of the user for whom you want to grant access to the system agent. The name must be a minimum of eight characters.
4. Select either read-only or read-write access for this user.
5. To authenticate the user, select **Authentication**.
   a. Select either the MD5 or the SHA1 protocol.
   b. Enter the authentication key in the **Key** text field.
   c. To provide encryption to the authentication session, select **Privacy**.
   d. Select either the AES or the DES protocol.

e. Enter the encryption key in the **Key** text field.

6. Click **OK**.

The newly added user account appears in the SNMP Users table.

Modifying SNMP V3 users

You can modify the access level (read-only or read-write) and authentication protocol for existing SNMPv3 users.

Procedure

1. Select **Administration** > **Settings** > **SNMP**.
2. In the **SNMP Users** area, select a checkbox for the user and click **Modify**.

   The Modify SNMP User dialog box appears. Add or change any of the following settings.

3. Select either read-only or read-write access for this user.
4. To authenticate the user, select **Authentication**.
   a. Select either the MD5 or the SHA1 protocol.
   b. Enter the authentication key in the Key text field.
   c. To provide encryption to the authentication session, select **Privacy**.
   d. Select either the AES or the DES protocol.
   e. Enter the encryption key in the **Key** text field.
5. Click **OK**.

   The new settings for this user account appear in the SNMP Users table.

Removing SNMP V3 users

Use the SNMP tab to delete existing SNMPv3 users.

Procedure

1. Select **Administration** > **Settings** > **SNMP**.
2. In the SNMP Users area, select a checkbox for the user and click **Delete**.

   The Delete SNMP User dialog box appears.

   Note: If the **Delete** button is disabled, the selected user is being used by one or more trap hosts. Delete the trap hosts and then delete the user.

3. Verify the user name to be deleted and click **OK**.
4. In the Delete SNMP User Status dialog box, click **Close**.

   The user account is removed from the SNMP Users table.

SNMP V2C community management

Define SNMP v2c communities (which serve as passwords) to control management system access to the protection system. To restrict access to specific hosts that use the specified community, assign the hosts to the community.

Note: The SNMP V2c Community string is a sent in cleartext and is very easy to intercept. If this occurs, the interceptor can retrieve information from devices on your network, modify their configuration, and possibly shut them down. SNMP V3 provides authentication and encryption features to prevent interception.

Note: SNMP community definitions do not enable the transmission of SNMP traps to a management station. You must define trap hosts to enable trap submission to management stations.

Creating SNMP V2C communities

Create communities to restrict access to the DDR system or for use in sending traps to a trap host. You must create a community and assign it to a host before you can select that community for use with the trap host.

Procedure

1. Select **Administration** > **Settings** > **SNMP**.
2. In the Communities area, click **Create**.

   The Create SNMP V2C Community dialog box appears.
3. In the **Community** box, enter the name of a community for whom you want to grant access to the system agent.
4. Select either read-only or read-write access for this community.
5. If you want to associate the community to one or more hosts, add the hosts as follows:
   a. Click + to add a host.

      The Host dialog box appears.

   b. In the **Host** text field, enter the IP address or domain name of the host.

   c. Click **OK**.

      The Host is added to the host list.
6. Click **OK**.

   The new community entry appears in the **Communities** table and lists the selected hosts.

Modifying SNMP V2C Communities

Procedure

1. Select **Administration** > **Settings** > **SNMP**.
2. In the Communities area, select the checkbox for the community and click **Modify**.

   The Modify SNMP V2C Community dialog box appears.
3. To change the access mode for this community, select either **read-only** or **read-write** access.

Note: The Access buttons for the selected community are disabled when a trap host on the same system is configured as part of that community. To modify the access setting, delete the trap host and add it back after the community is modified.

4. To add one or more hosts to this community, do the following:
   a. Click + to add a host.

      The Host dialog box appears.

   b. In the **Host** text field, enter the IP address or domain name of the host.
   c. Click **OK**.

      The Host is added to the host list.
5. To delete one or more hosts from the host list, do the following:

   Note: DD System Manager does not allow you to delete a host when a trap host on the same system is configured as part of that community. To delete a trap host from a community, delete the trap host and add it back after the community is modified.

   Note: The Access buttons for the selected community are not disabled when the trap host uses an IPv6 address and the system is managed by an earlier DD OS version that does not support IPv6. If possible, always select a management system that uses the same or a newer DD OS version than the systems it manages.

   a. Select the checkbox for each host or click the Host check box in the table head to select all listed hosts.
   b. Click the delete button (X).
6. To edit a host name, do the following:
   a. Select the checkbox for the host.
   b. Click the edit button (pencil icon).
   c. Edit the host name.
   d. Click **OK**.
7. Click **OK**.

   The modified community entry appears in the Communities table.

Deleting SNMP V2C communities

Use the SNMP tab to delete existing SNMPv2 communities.

Procedure

1. Select **Administration** > **Settings** > **SNMP**.
2. In the **Communities** area, select a checkbox for the community and click **Delete**.

   The Delete SNMP V2C Communities dialog box appears.

   Note: If the **Delete** button is disabled, the selected community is being used by one or more trap hosts. Delete the trap hosts and then delete the community.

3. Verify the community name to be deleted and click **OK**.
4. In the Delete SNMP V2C Communities Status dialog box, click **Close**. The community entry is removed from the Communities table.

SNMP trap host management

Trap host definitions enable protection systems to send alert messages in SNMP trap messages to an SNMP management station.

Creating SNMP V3 and V2C trap hosts

Trap host definitions identify remote hosts that receive SNMP trap messages from the system.

Before you begin

If you plan to assign an existing SNMP v2c community to a trap host, you must first use the Communities area to assign the trap host to the community.

Procedure

1. Select **Administration** > **Settings** > **SNMP**.
2. In the SNMP V3 Trap Hosts or SNMP V2C Trap Hosts area, click **Create**.

   The Create SNMP [V3 or V2C] Trap Hosts dialog appears.
3. In the **Host** box, enter the IP address or domain name of the SNMP Host to receive traps.
4. In the **Port** box, enter the port number for sending traps (port 162 is a common port).
5. Select the user (SNMP V3) or the community (SNMP V2C) from the drop-down menu.

   Note: The Community list displays only those communities to which the trap host is already assigned.
6. To create a new community, do the following:
   a. Select **Create New Community** in the Community drop-down menu.
   b. Enter the name for the new community in the **Community** box.
   c. Select the Access type.
   d. Click the add (+) button.
   e. Enter the trap host name.
   f. Click **OK**.
   g. Click **OK**.
7. Click **OK**.

Modifying SNMP V3 and V2C trap hosts

You can modify the port number and community selection for existing trap host configurations.

Procedure

1. Select **Administration** > **Settings** > **SNMP**.
2. In the **SNMP V3 Trap Hosts** or **SNMP V2C Trap Hosts** area, select a Trap Host entry, and click **Modify**.

   The Modify SNMP [V3 or V2C] Trap Hosts dialog box appears.
3. To modify the port number, enter a new port number in the **Port** box (port 162 is a common port).
4. Select the user (SNMP V3) or the community (SNMP V2C) from the drop-down menu.

> Note: The Community list displays only those communities to which the trap host is already assigned.

5. To create a new community, do the following:
   a. Select **Create New Community** in the Community drop-down menu.
   b. Enter the name for the new community in the **Community** box.
   c. Select the Access type.
   d. Click the add (+) button.
   e. Enter the trap host name.
   f. Click **OK**.
   g. Click **OK**.
6. Click **OK**.

Removing SNMP V3 and V2C trap hosts

Use the SNMP tab to delete existing trap host configurations.

Procedure

1. Select **Administration** > **Settings** > **SNMP**.
2. In the **Trap Hosts** area (either for V3 or V2C, select a checkbox for the trap host and click **Delete**.

   The Delete SNMP [V3 or V2C] Trap Hosts dialog box appears.
3. Verify the host name to be deleted and click **OK**.
4. In the Delete SNMP [V3 or V2C] Trap Hosts Status dialog box, click **Close**.

   The trap host entry is removed from the **Trap Hosts** table.

Autosupport report management

The Autosupport feature generates a report that is called an Auto Support log (ASUP). The ASUP shows system identification information, consolidated output from several system commands, and entries from various log files. Extensive and detailed internal statistics appear at the end of the report. This report is designed to aid Support in debugging system problems.

An ASUP is generated as scheduled, which is usually once per day. Additionally, every time the file system starts, the system generates a new ASUP.

Other reports are triggered by system events such as alerts, and are more limited in scope. They contain basic system information, and information about the event that triggered the report.

You can configure email addresses to receive the daily ASUP reports, and you can enable or disable sending of these reports to Dell EMC. The default time for sending the daily ASUP is 06.00 a.m, and it is configurable. When sending ASUPs to Dell EMC you have the option to select the legacy unsecure method or the ConnectEMC method, which encrypts the information before transmission.

Setup sending ASUP using the GUI

If the system is not configured to send ASUPs to Dell EMC Support, perform these tasks from the GUI.

Configure mail server settings

To configure a mail server:

1. Click **System Settings** > **General Configuration** > **Mail Server tabs**.
2. From the **More Tasks** menu, select **Set Mail Server**. The **Set Mail Server** dialog box opens.
3. In the **Mail Server** text box, enter the name of the mail server.
4. Click **OK**.

View Autosupport email list

1. Select the system in the Navigational pane.
2. Click the **Maintenance** > **Support** tabs. The configured emails for the autosupport email list are shown below the Detailed Autosupport Mailing List area.

Configure the Autosupport Mailing List

To receive emails for autosupport reports, add a recipients email address to the email list. It is recommended to test the setup to ensure that messages are received. To set the list of email addresses receiving autosupport notification:

ⓘ Note: In order for Auto Support to send to Dell EMC, you must add the following account: autosupport@autosupport.datadomain.com

1. Click the **Maintenance** > **Support** tabs.
2. Click **Add** or **Modify** next to the **Detailed Autosupport Mailing List**. The **Add or Modify Detailed Autosupport Mailing Lists** dialog box opens.
3. In the **Email** area, click the **+** (plus) icon. The **Email** dialog box opens.
4. Enter the recipients email address in the **Autosupport Email** text box.
5. Click **OK**. The new autosupport email addresses open in the **Detailed Autosupport Mailing Lists** area.

Test the Alerts Email List

The addresses should be tested to ensure that they are receiving mail after configuring the email lists. To test newly added alerts emails:

1. Click the **Status** > **Alerts** > **Notification** tabs.
2. Select **Send Test Alert** from the **More Tasks** menu. The **Send Test Alert** dialog box opens.
3. In the **Notification Groups** area, select the checkboxes of groups to send test emails and click **Next**.
4. Optionally, add or create other email addresses.
5. Click **Send Now** and **OK**. To test newly added autosupport emails for mailer problems, use the autosupport test command autosupport test email email-addr For example, after adding the email address `abc@yourcompany.com` to the list, check the address with the command: `autosupport test`.

HA system autosupport and support bundle manageability

Configuration is done on the active node and mirrored to the standby node; therefore, the same configuration is on both nodes, but there is not a consolidated ASUP and support bundle.

Autosupport and support bundle on the active node also includes filesystem, replication, protocol, and full HA information in addition to local node information. Autosupport and support bundle on the standby node only have local node information plus some HA information (configuration and status), but no filesystem/replication/protocol information. The autosupports and support bundles from both the nodes will be needed to debug issues related to HA system status (filesystem, replication, protocols, and HA configuration).

Enabling and disabling autosupport reporting to Dell EMC

You can enable or disable autosupport reporting to Dell EMC without affecting whether or not alerts are sent to Dell EMC.

Procedure

1. To view the autosupport reporting status, select **Maintenance** > **Support** > **Autosupport**.

   The autosupport reporting status is highlighted next to the Scheduled autosupport label in the Support area. Depending on the current configuration, either an **Enable** or a **Disable** button appears in the Scheduled autosupport row.
2. To enable autosupport reporting, click **Enable** in the Scheduled autosupport row.
3. To disable autosupport reporting, click **Disable** in the Scheduled autosupport row.

Reviewing generated autosupport reports

Review autosupport reports to view system statistics and configuration information captured in the past. The system stores a maximum of 14 autosupport reports.

Procedure

1. Select **Maintenance** > **Support** > **Autosupport**.

   The Autosupport Reports page shows the autosupport report file name and file size, and the date the report was generated. Reports are automatically named. The most current report is autosupport, the previous day is autosupport.1, and the number increments as the reports move back in time.
2. Click the file name link to view the report using a text editor. If doing so is required by your browser, download the file first.

Configuring the autosupport mailing list

Autosupport mailing list subscribers receive autosupport messages through email. Use the Autosupport tab to add, modify, and delete subscribers.

About this task

Autosupport emails are sent through the configured mail server to all subscribers in the autosupport email list. After you configure the mail server and autosupport email list, it is a good practice to test the setup to ensure that autosupport messages reach the intended destinations.

Procedure

1. Select **Maintenance** > **Support** > **Autosupport**.
2. Click **Configure**.

   The Configure Autosupport Subscribers dialog box appears.

3. To add a subscriber, do the following.
   a. Click Add (+).
      The Email dialog box appears.
   b. Enter the recipients email address in the Email box.
   c. Click OK.

   CLI equivalent

   ```
   # autosupport add asup-detailed emails djones@company.com
   # autosupport add alert-summary emails djones@company.com
   ```

4. To delete a subscriber, do the following.
   a. In the Configure Autosupport Subscribers dialog box, select the subscriber to delete.
   b. Click Delete (**X**).

   CLI equivalent

   ```
   # autosupport del asup-detailed emails djones@company.com
   # autosupport del alert-summary emails djones@company.com
   ```

5. To modify a subscriber email address, do the following.
   a. In the Configure Autosupport Subscribers dialog box, select the subscriber name to edit.
   b. Click Modify (pencil icon).
      The Email dialog box appears.
   c. Modify the email address as needed.
   d. Click OK.
6. Click **OK** to close the Configure Autosupport Subscribers dialog box.
   The revised autosupport email list appears in the Autosupport Mailing List area.

Verifying the system is able to send ASUP and alert emails to external recipients

Confirm that external email recipients can receive the autosupport (ASUP) and alert emails you send from your protection system.

About this task

Verify autosupport (ASUP) is getting relayed by the exchange server.

Procedure

1. Check if ASUPs can be sent to a local email address, an email address on the same Mail Server.

   ```
   # autosupport send [internal-email-addr]
   ```

2. Check if ASUPs can be sent to an email address outside the local mail server.

   ```
   # autosupport send [external email-addr]
   ```

3. If the email does not get to the external email address on the mail server, you may receive an error such as:

```
**** Unable to send message: (errno 51: Unrecoverable errors from server--
giving up)
```

   In this case, it is likely that forwarding will need to be enabled for the system on the local mail server by using the steps outlined in the KB article *Configure Email Relay on MS Exchange*, available at https://support.emc.com/kb/181900.

4. If the ASUP can be sent to an external email address, but is not getting to Dell EMC, there may be an issue with the firewall configuration or spam filters.

Support bundle management

A support bundle is a file that contains system configuration and operation information. It is a good practice to generate a support bundle before a software upgrade or a system topology change (such as a controller upgrade).

Dell EMC Support often requests a support bundle when providing assistance.

The KB articles *How to collect/upload a support bundle (SUB) from a Data Domain Restorer (DDR)*, available at https://support.emc.com/kb/180563 and Gathering Autosupports, provide additional information about gathering and working with support bundles.

Generating a support bundle

When troubleshooting problems, Dell EMC Support may ask for a support bundle, which is a tar-g-zipped selection of log files with a README file that includes identifying autosupport headers.

Procedure

1. Select **Maintenance** > **Support** > **Support Bundles**.
2. Click **Generate Support Bundle**.

   Note: The system supports a maximum of five support bundles. If you attempt to generate an sixth support bundle, the system automatically deletes the oldest support bundle. You can also delete support bundles using the CLI command `support bundle delete`.

   Also, if you generate a support bundle on a upgraded system that contains a support bundle named using the old format, `support-bundle.tar.gz`, that file is renamed to use the newer name format.

3. Email the file to customer support at support@emc.com.

   Note: If the bundle is too large to be emailed, use the online support site to upload the bundle. (Go to https://support.emc.com.)

Generating a mini support bundle

If the support bundle is too large, DD OS provides the ability to create a mini bundle that is smaller in size.

About this task

For automatically generated mini support bundles, the maximum number allowed is two created within the last 24 hours, and four total. New mini bundles will not be generated if there are already two that were created in the last 24 hours. If the maximum of four is reached, the system will automatically delete the oldest one.

Procedure

1. Select **Maintenance** > **Support** > **Support Bundles**.
2. Click **Generate Mini Support Bundle**.

   Note: The system supports a maximum of five support bundles (standard and mini). If you attempt to generate an sixth support bundle, the system automatically deletes the oldest support bundle. You can also delete support bundles using the CLI command `support bundle delete`.

3. Email the file to customer support at support@emc.com.

   Note: If the bundle is too large to be emailed, use the online support site to upload the bundle. (Go to https://support.emc.com.)

Viewing the support bundles list

Use the Support Bundles tab to view the support bundle files on the system.

Procedure

1. Select **Maintenance** > **Support** > **Support Bundles**.
   The Support Bundles list appears.

   Listed are the support bundle file name, file size, and date the bundle was generated. Bundles are automatically named `hostname-support-bundle-datestamp.tar.gz`. An example filename is `localhost-support-bundle-1127103633.tar.gz`, which indicates that the support bundle was created on the localhost system on November 27th at 10:36:33.

2. Click the file name link and select a gz/tar decompression tool to view the ASCII contents of the bundle.

Coredump management

A core is a file that contains details about the specific problem encountered when the protection system suffers a crash due to a coredump. DD OS keeps a record of these files to assist with troubleshooting.

Navigate to **Maintenance** > **Support** > **Cores**.

If a core file is too big, DD OS provides the ability to split it into smaller chunks. Split files are automatically deleted after 48 hours.

The table provides the following information about the core files that exist on the system:

Item	Description
File Name	Name of the core file.
Type	Whether the core file is a full core, or a chunk from a core file that was split.
Size	Size of the core file.
Created On	Date the core file was created.

Splitting a coredump file

When DD OS crashes due to a coredump, a core file describing the problem is created in the `/ddvar/core` directory. This file may be large, and difficult to copy off the protection system. If

the core file cannot be copied off the system because it is too large, DD OS provides the ability to split the core file into smaller chunks.

Procedure

1. Select **Maintenance** > **Support** > **Cores**.
2. Select a core file from the table.
3. Click **Split**.
4. In the **Size** field, specify the size of the chunks to create and select **MiB** or **GiB** from the list box.

   Note: A single core file can be broken down into a maximum of 20 chunks. The command will fail with an error if the specified size would result in more than 20 chunks.

5. Click **OK**.

Results

DD OS splits the selected coredump file into chunks of the specified size, and places them in the `/ddvar/core` directory. Split files are automatically deleted after 48 hours.

CLI equivalent

Procedure

1. Run the `support coredump split <filename> <n> (MiB|GiB)` command, where:
   - *<filename>* is the name of the core file in the `/ddvar/core` directory
   - *<n>* is the size of the smaller chunks to create

     Note: A single core file can be broken down into a maximum of 20 chunks. The command will fail with an error if the specified size would result in more than 20 chunks.

   For example, splitting a 42.1 MB core file named `cpmdb.core.19297.1517443767` into 10 MB chunks would result in five chunks.

```
# support coredump split cpmdb.core.19297.1517443767 10 MiB
cpmdb.core.19297.1517443767 will be split into 5 chunks.
Splitting...

The md5 and split chunks of cpmdb.core.19297.1517443767:
File                                Size       Time Created
----------------------------------  --------   ------------------------
cpmdb.core.19297.1517443767_5_01    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_02    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_03    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_04    10.0 MiB   Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767_5_05    2.1 MiB    Mon Feb  5 11:50:57 2018
cpmdb.core.19297.1517443767.md5     0 MiB      Mon Feb  5 11:50:58 2018
----------------------------------  --------   ------------------------
Download the files as soon as possible. Otherwise they will be automatically delete in 48
hours.
```

2. Run the `support coredump save <file-list>` command to save specified coredump files to a USB drive. Split files are automatically deleted after 48 hours.

Alert notification management

The alert feature generates event and summary reports that can be distributed to configurable email lists and to Dell EMC.

Event reports are sent immediately and provide detailed information on a system event. The distribution lists for event alerts are called *notification groups*. You can configure a notification

group to include one or more email addresses, and you can configure the types and severity level of the event reports sent to those addresses. For example, you might configure one notification group for individuals who need to know about critical events and another group for those who monitor less critical events. Another option is to configure groups for different technologies. For example, you might configure one notification group to receive email messages about all network events and another group to receive messages about storage issues.

Summary reports are sent daily and provide a summary of the events that occurred during the last 24 hours. Summary reports do not include all the information that is provided in event reports. The default generation time for the daily report is 08.00 a.m, and it can be changed. Summary reports are sent using a dedicated email list that is separate from the event notification groups.

You can enable or disable alert distribution to Dell EMC. When sending reports to Dell EMC, you have the option to select the legacy unsecure method or Secure Remote Services for secure transmissions.

HA system alert notification management

The alert feature on an HA system generates event and summary report like a non-HA system but how the HA system manages these alerts is different due to the two node system set-up.

Initial alert configuration is completed on the active node and mirrored to the stand-by (i.e., same configuration on both nodes). Local and AM-Alerts are emailed according to the notification settings and include information indicating they are from an HA system and from which node, the active or standby, that generated the alerts.

If there are active alerts on the file system, replication, or protocols when a failover occurs, these active alerts continue to show on the new active node after failover if the alert conditions have not cleared up.

Historical alerts on the filesystem, replication, and protocols stay with the node where they originated rather than failing over together with the filesystem on a failover. This means the CLIs on the active node will not present a complete/continuous view of historical alerts for filesystem, replication, and protocols

During a failover, local historical alerts stay with the node from which they were generated; however, the historical alerts for the filesystem, replication, and protocols (generally called "logical alerts") fail over together with the filesystem.

Note: The **Health** > **High Availability** panel displays only alerts that are HA-related. Those alerts can be filtered by major HA component, such as HA Manager, Node, Interconnect, Storage, and SAS connection.

Viewing the notification group list

A notification group defines a set of alert types (classes) and a group of email addresses (for subscribers). Whenever the system generates an alert type selected in a notification list, that alert is sent to the list subscribers.

Procedure

1. Select **Health** > **Alerts** > **Notification**.

   CLI equivalent

   ```
   # alerts notify-list show
   ```

2. To limit (filter) the entries in the Group Name list, type a group name in the Group Name box or a subscriber email in the Alert Email box, and click **Update**.

   Note: Click **Reset** to display all configured groups.

3. To display detailed information for a group, select the group in the Group Name list.

Notification tab

The Notification tab allows you to configure groups of email address that receive system alerts for the alert types and severity levels you select.

Table 39 Group Name list, column label descriptions

Item	Description
Group Name	The configured name for the group.
Classes	The number of alert classes that are reported to the group.
Subscribers	The number of subscribers who are configured to receive notifications through email.

Table 40 Detailed Information, label descriptions

Item	Description
Class	A service or subsystem that can forward alerts. The listed classes are those for which the notification group receives alerts.
Severity	The severity level that triggers an email to the notification group. All alerts at the specified severity level and above are sent to the notification group.
Subscribers	The subscribers area displays a list of all email addresses configured for the notification group.

Table 41 Notification tab controls

Control	Description
Add button	Click the **Add** button to begin creating a notification group.
Class Attributes Configure button	Click this Configure button to change the classes and severity levels that generate alerts for the selected notification group.
Delete button	Click the **Delete** button to delete the selected notification group.
Filter By: Alert Email box	Enter text in this box to limit the group name list entries to groups that include an email address that contains the specified text.
Filter By: Group Name box	Enter text in this box to limit the group name list entries to group names that contain the specified text.
Modify button	Click the **Modify** button to modify the configuration for the selected notification group.
Reset button	Click this button to remove any entries in the Filter By boxes and display all group names.

Table 41 Notification tab controls (continued)

Control	Description
Subscribers Configure button	Click this Configure button to change the email list for the selected notification group.
Update button	Click this button to update the group name list after you enter text in a filter box.

Creating a notification group

Use the Notification tab to add notification groups and select the severity level for each group.

Procedure

1. Select **Health** > **Alerts** > **Notification**.
2. Click **Add**.

   The Add Group dialog box appears.

3. Type the group name in the **Group Name** box.
4. Select the checkbox of one or more alert classes of which to be notified.
5. To change the default severity level (Warning) for a class, select another level in the associated list box.

   The severity levels are listed in ascending severity level. *Emergency* is the highest severity level.

6. Click **OK**.

   CLI equivalent

   ```
   # alerts notify-list create eng_grp class hardwareFailure
   ```

Managing the subscriber list for a group

Use the Notification tab to add, modify, or delete email addresses from a notification group subscriber list.

Procedure

1. Select **Health** > **Alerts** > **Notification**.
2. Select the checkbox of a group in the Notifications group list, and do one of the following.
   - Click **Modify** and select **Subscribers**.
   - Click **Configure** in the Subscribers list.
3. To add a subscriber to the group, do the following.

   a. Click the + icon.

   The Email Address dialog box appears.

   b. Enter the email address of a subscriber.

   c. Click **OK**.

   CLI equivalent

```
# alerts notify-list add eng_lab emails
mlee@urcompany.com,bob@urcompany.com
```

4. To modify an email address, do the following.
   a. Click the checkbox of the email address in the **Subscriber Email** list.
   b. Click the pencil icon.
   c. Edit the email address in the Email Address dialog box.
   d. Click **OK**.
5. To delete an email address, click the checkbox of the email address in the **Subscriber Email** list and click the **X** icon.

   CLI equivalent

   ```
   # alerts notify-list del eng_lab emails bob@urcompany.com
   ```

6. Click **Finish** or **OK**.

Modifying a notification group

Use the Notification table to modify the attribute classes in an existing group.

Procedure

1. Select **Health** > **Alerts** > **Notification**.
2. Select the checkbox of the group to modify in the group list.
3. To modify the class attributes for a group, do the following.
   a. Click **Configure** in the Class Attributes area.

      The Edit Group dialog box appears.
   b. Select (or clear) the checkbox of one or more class attributes.
   c. To change the severity level for a class attribute, select a level from the corresponding list box.
   d. Click **OK**.

      CLI equivalent

      ```
      # alerts notify-list add eng_lab class cloud severity warning
      # alerts notify-list del eng_lab class cloud severity notice
      ```

4. To modify the subscriber list for a group, do the following.
   a. Click **Configure** in the Subscribers area.

      The Edit Subscribers dialog box appears.
   b. To delete subscribers from the group list, select the checkboxes of subscribers to delete and click the Delete icon (X).
   c. To add a subscriber, click the Add icon (+), type a subscriber email address, and click OK.
   d. Click **OK**.

      CLI equivalent

      ```
      # alerts notify-list add eng_lab emails
      ```

```
mlee@urcompany.com,bob@urcompany.com
# alerts notify-list del eng_lab emails bob@urcompany.com
```

5. Click **OK**.

Deleting a notification group

Use the Notification tab to delete one or more existing notification groups.

Procedure

1. Select **Health** > **Alerts** > **Notification**.
2. Select one or more checkboxes of groups in the Notifications group list, and click **Delete**.

   The Delete Group dialog box appears.

3. Verify the deletion and click **OK**.

   CLI equivalent

   ```
   # alerts notify-list destroy eng_grp
   ```

Resetting the notification group configuration

Use the Notification tab to remove all notification groups added and to remove any changes made to the Default group.

Procedure

1. Select **Health** > **Alerts** > **Notification**.
2. Select **More Tasks** > **Reset Notification Groups**.
3. In the Reset Notification Groups dialog box, click **Yes** in the verification dialog.

   CLI equivalent

   ```
   # alerts notify-list reset
   ```

Configuring the daily summary schedule and distribution list

Every day, each managed system sends a Daily Alert Summary email to the subscribers configured for the alertssummary.list email group. The Daily Alert Summary email contains current and historical alerts showing messages about non-critical hardware situations and disk space usage numbers that you might want to address soon.

About this task

A fan failure is an example of a noncritical issue that you might want to address as soon as is reasonably possible. When Support receives the failure notification, they contact you to arrange for component replacement.

Procedure

1. Select **Health** > **Alerts** > **Daily Alert Summary**.
2. If the default deliver time of 8 AM is not acceptable, do the following.

   a. Click **Schedule**.

   The Schedule Alert Summary dialog box appears.

b. Use the list boxes to select the hour, minute, and either AM or PM for the summary report.

c. Click **OK**.

CLI equivalent

```
# autosupport set schedule alert-summary daily 1400
```

3. To configure the daily alert subscriber list, do the following.

a. Click **Configure**.

The Daily Alert Summary Mailing List dialog box appears.

b. Modify the daily alert subscriber list as follows.

- To add a subscriber, click the + icon, type the email address, and click **OK**.
  CLI equivalent

  ```
  # autosupport add alert-summary emails djones@company.com
  ```
- To modify an email address, select the checkbox for the subscriber, click the pencil icon, edit the email address, and click **OK**.
- To delete an email address, select the checkbox for the subscriber and click **X**.
  CLI equivalent

  ```
  # autosupport del alert-summary emails djones@company.com
  ```

c. Click **Finish**.

Daily Alert Summary tab

The Daily Alert Summary tab allows you to configure an email list of those who want to receive a summary of all system alerts once each day. The people on this list do not receive individual alerts unless they are also added to a notification group.

Table 42 Daily Alert Summary, label descriptions

Item	Description
Delivery Time	The delivery time shows the configured time for daily emails.
Email List	This list displays the email addresses of those who receive the daily emails.

Table 43 Daily Alert Summary tab controls

Control	Description
Configure button	Click the **Configure** button to edit the subscriber email list.
Schedule button	Click the **Schedule** button to configure the time that the daily report is sent.

Enabling and disabling alert notification to Dell EMC

You can enable or disable alert notification to Dell EMC without affecting whether or not autosupport reports are sent to Dell EMC.

Procedure

1. To view the alert reporting status, select **Maintenance** > **Support** > **Autosupport**.

   The alert notification status is highlighted in green next to the Real-time alert label in the Support area. Depending on the current configuration, either an **Enable** or a **Disable** button appears in the Real-time alert row.
2. To enable alert reporting, click **Enable** in the Real-time alert row.
3. To disable alert reporting, click **Disable** in the Real-time alert row.

Testing the alerts email feature

Use the Notification tab to send a test email to select notification groups or email addresses. This feature allows you to determine if the system is configured correctly to send alert messages.

Procedure

1. To control whether or not a test alert is sent to Dell EMC, do the following.
   a. Select **Maintenance** > **Support** > **Autosupport**.
   b. In the **Alert Support** area, click **Enable** or **Disable** to control whether or not the test email is sent .

      You cannot change the email address.
2. Select **Health** > **Alerts** > **Notification**.
3. Select **More Tasks** > **Send Test Alert**.

   The Send Test Alert dialog box appears.
4. In the **Notification Groups** list, select groups to receive the test email and click **Next**.
5. Optionally, add additional email addresses to receive the email.
6. Click **Send Now** and **OK**.

   CLI equivalent

   ```
   # alerts notify-list test jsmith@yourcompany.com
   ```
7. If you disabled sending of the test alert to Dell EMC and you want to enable this feature now, do the following.
   a. Select **Maintenance** > **Support** > **Autosupport**.
   b. In the **Alert Support** area, click **Enable** .

Results

To test newly added alerts emails for mailer problems, enter: `autosupport test email` *email-addr*

For example, after adding the email address djones@yourcompany.com to the list, check the address with the command: `autosupport test email` *djones@yourcompany.com*

Support delivery management

Delivery management defines how alerts and autosupport reports are sent to Dell EMC. By default, alerts and autosupport reports are sent to Dell EMC Support using the standard (unsecure) email. The ConnectEMC method sends messages in a secure format through the Secure Remote Services Virtual Edition (VE) gateway.

When the ConnectEMC method is used with a Secure Remote Services gateway, one benefit is that one gateway can forward messages from multiple systems, and this allows you to configure network security for only the Secure Remote Services gateway instead of for multiple systems. Also, a usage intelligence report is generated and sent if electronic licenses are adopted.

When configuring a Secure Remote Services gateway, the protection system supports registering multiple gateways to provide redundancy.

Selecting standard email delivery to Dell EMC

When you select the standard (non-secure) email delivery method, this method applies to both alert and autosupport reporting.

Procedure

1. Select **Maintenance** > **Support** > **Autosupport**.
2. Click **Configure** in the Channel row in the Support area.

   The Configure EMC Support Delivery dialog appears. The delivery method is displayed after the Channel label in the Support area.
3. In the **Channel** list box, select **Email to datadomain.com**.
4. Click **OK**.

   CLI equivalent

   ```
   # support notification method set email
   ```

Selecting and configuring Secure Remote Services delivery

Secure Remote Services Virtual Edition (VE) Gateway provides automated connect home and remote support activities through an IP-based solution that is enhanced by a comprehensive security system.

About this task

An on-premise Secure Remote Services version 3 gateway provides the ability to monitor both on-premise protection systems and DDVE instances, and cloud-based DDVE instances.

Procedure

1. Select **Maintenance** > **Support** > **Autosupport**.
2. Click **Configure** in the Channel row in the Support area.

   The Configure Dell EMC Support Delivery dialog box appears. The delivery method is displayed after the Channel label in the Support area.
3. In the **Channel** list box, select **Secure Remote Services**.
4. Type the gateway hostname and select the local IP address for the system.
5. Click **OK**.

6. Type the service link username and password.
7. Click **Register**.

   Secure Remote Services details are displayed in the Autosupport panel.

CLI equivalent

Procedure

1. To set up the administrator email, enter:

```
# config set admin-email dd_admin1@emc.com
The Admin Email is: dd_admin1@emc.com
```

2. To register the system to the ESRS-gateway (Secure Remote Services), enter:

```
# support connectemc device register ipaddr esrs-gateway [host-list] [ha-peer ipaddr]
```

> CAUTION When configuring Secure Remove Services delivery on an HA pair:
>
> - The `ha-peer` parameter is required when configuring Secure Remote Services on HA pairs to register both nodes.
> - The customer must provide Service Link credentials to run the `support connectemc device register` command on an HA pair, because attempting to register the HA pair as a user will fail and cause the RSA key token to become out of synch.

3. To enable the sending of autosupports, enter:

```
# support notification enable all
Enabled sending autosupport and alerts to EMC.
```

4. To set the notification method to ConnectEMC, enter:

```
# support notification method set connectemc
Support notification method set to "connectemc".
```

5. To show the notification setup, enter:

```
# support notification show all
Notification   Status    Destination
------------   -------   ----------------------
alerts         enabled   ftp://111.111.11.111:11
autosupport    enabled   ftp://111.111.11.111:11
------------   -------   ----------------------
```

6. To show the notification setup, enter:

```
# support connectemc config show
ConnectEMC configuration:
        ESRS gateway IP/hostname:          esrs-gateway.datadomain.com
        Registered device IP(s)            10.25.246.70
```

Testing ConnectEMC operation

A CLI command allows you to test ConnectEMC operation by sending a test message to Support through the Secure Remote Services gateway.

Procedure

1. To test ConnectEMC operation, use the CLI.

```
#support connectemc test
Sending test message through ConnectEMC...
Test message successfully sent through ConnectEMC.
```

Log file management

The protection system maintains a set of log files, which can be bundled and sent to Support to assist in troubleshooting any system issues that may arise. Log files cannot be modified or deleted by any user with DD System Manager, but they can be copied from the log directory and managed off of the system.

Note: Log messages on an HA system are preserved on the node where the log file originated.

Log files are rotated weekly. Every Sunday at 0:45 a.m., the system automatically opens new log files for the existing logs and renames the previous files with appended numbers. For example, after the first week of operation, the previous week `messages` file is renamed `messages.1`, and new messages are stored in a new messages file. Each numbered file is rolled to the next number each week. For example, after the second week, the file `messages.1` is rolled to `messages.2`. If a `messages.2` file already existed, it rolls to `messages.3`. At the end of the retention period (shown in the table below, the expired log is deleted. For example, an existing `messages.9` file is deleted when `messages.8` rolls to `messages.9`.

The `audit.log` does not rotate on a weekly basis. Instead, it rotates when the file reaches 70 MB in size.

Except as noted in this topic, the log files are stored in `/ddvar/log`.

Note: Files in the `/ddvar` directory can be deleted using Linux commands if the Linux user is assigned *write* permission for that directory.

The set of log files on each system is determined by the features configured on the system and the events that occur. The following table describes the log files that the system can generate.

Table 44 System log files

Log File	Description	Retention Period
audit.log	Messages about user log-in events.	15 weeks
cifs.log	Log messages from the CIFS subsystem are logged only in `debug/cifs/cifs.log`. Size limit of 50 MiB.	10 weeks
messages	Messages about general system events, including commands executed.	9 weeks
secure.log	Messages regarding user events such as successful and failed logins, user additions and deletions, and password changes. Only Admin role users can view this file.	9 weeks
space.log	Messages about disk space usage by system components, and messages from the clean process. A space use message is generated every hour. Each time the clean process runs, it creates approximately 100 messages. All messages are in comma-separated-value format with tags you can use to separate the disk space messages from the clean process messages. You can use third-party software to analyze either set of messages. The log file uses the following tags. • CLEAN for data lines from clean operations. • CLEAN_HEADER for lines that contain headers for the clean operations data lines.	A single file is kept permanently. There is no log file rotation for this log.

Table 44 System log files (continued)

Log File	Description	Retention Period
	• SPACE for disk space data lines. • SPACE_HEADER for lines that contain headers for the disk space data lines.	

Viewing log files in DD System Manager

Use the Logs tab to view and open the system log files in DD System Manager.

Procedure

1. Select **Maintenance** > **Logs**.

   The Logs list displays log file names and the size and generation date for each log file.

2. Click a log file name to view its contents. You may be prompted to select an application, such as Notepad.exe, to open the file.

Displaying a log file in the CLI

Use the `log view` command to view a log file in the CLI.

Procedure

1. To view a log file in the CLI, use the `log view` command.

   With no argument, the command displays the current messeges file.

2. When viewing the log, use the up and down arrows to scroll through the file; use the q key to quit; and enter a slash character (/) and a pattern to search through the file.

The display of the messages file is similar to the following. The last message in the example is an hourly system status message that the protection system generates automatically. The message reports system uptime, the amount of data stored, NFS operations, and the amount of disk space used for data storage (%). The hourly messages go to the system log and to the serial console if one is attached.

```
# log view
Jun 27 12:11:33 localhost rpc.mountd: authenticated unmount
request from perfsun-g.emc.com:668 for /ddr/col1/segfs (/ddr/
col1/segfs)

Jun 27 12:28:54 localhost sshd(pam_unix)[998]: session opened
for user jsmith10 by (uid=0)

Jun 27 13:00:00 localhost logger: at 1:00pm up 3 days, 3:42,
52324 NFS ops, 84763 GiB data col. (1%)
```

Note: GiB = Gibibytes = the binary equivalent of Gigabytes.

Learning more about log messages

Look up error messages in the Error Message Catalog for your DD OS version.

About this task

In the log file is text similar to the following.

```
Jan 31 10:28:11 syrah19 bootbin: NOTICE: MSG-SMTOOL-00006: No
replication throttle schedules found: setting throttle to unlimited.
```

The components of the message are as follows.

DateTime Host Process [PID]: **Severity**: MSG-**Module-MessageID: Message**

Severity levels, in descending order, are: Emergency, Alert, Critical, Error, Warning, Notice, Info, Debug.

Procedure

1. Go to the Online Support website at https://support.emc.com, enter *Error Message Catalog* in the search box, and click the search button.
2. In the results list, locate the catalog for your system and click on the link.
3. User your browser search tool to search for a unique text string in the message.

   The error message description looks similar to the following display.

   ```
   ID: MSG-SMTOOL-00006 - Severity: NOTICE - Audience: customer

   Message: No replication throttle schedules found: setting throttle
   to unlimited.

   Description: The restorer cannot find a replication throttle
   schedule. Replication is running with throttle set to unlimited.

   Action: To set a replication throttle schedule, run the
   replication throttle add command.
   ```

4. To resolve an issue, do the recommended action.

   Based on the example message description, one could run the `replication throttle add` command to set the throttle.

Saving a copy of log files

Save log file copies to another device when you want to archive those files.

About this task

Use NFS, CIFS mount, or FTP to copy the files to another machine. If using CIFS or NFS, mount /ddvar to your desktop and copy the files from the mount point. The following procedure describes how to use FTP to move files to another machine.

Procedure

1. On the protection system, use the `adminaccess show ftp` command to see whether FTP service is enabled. If the service is disabled, use the command `adminaccess enable ftp`.
2. Use the `adminaccess show ftp` command to see that the FTP access list includes the IP address of your remote machine. If the address is not in the list, use the command `adminaccess add ftp` *ipaddr*.

3. On the remote machine, open a web browser.
4. In the **Address** box at the top of the web browser, use FTP to access the protection system as shown in the following example.

   ```
   ftp://Data Domain system_name.yourcompany.com/
   ```

   Note: Some web browsers do not automatically ask for a login if a machine does not accept anonymous logins. In that case, add a user name and password to the FTP line. For example: `ftp://sysadmin:your-pw@Data Domain system_name.yourcompany.com/`

5. At the login pop-up, log into the protection system as user `sysadmin`.
6. On the protection system, you are in the directory just above the log directory. Open the log directory to list the messages files.
7. Copy the file that you want to save. Right-click the file icon and select **Copy To Folder** from the menu. Choose a location for the file copy.
8. If you want the FTP service disabled on the protection system, after completing the file copy, use SSH to log into the protection system as sysadmin and invoke the command `adminaccess disable ftp`.

Log message transmission to remote systems

Some log messages can be sent from the protection system to other systems. DD OS uses syslog to publish log messages to remote systems.

A protection system exports the following facility.priority selectors for log files. For information on managing the selectors and receiving messages on a third-party system, see your vendor-supplied documentation for the receiving system.

- *.notice—Sends all messages at the notice priority and higher.
- *.alert—Sends all messages at the alert priority and higher (alerts are included in *.notice).
- kern.*—Sends all kernel messages (kern.info log files).

The `log host` commands manage the process of sending log messages to another system.

Viewing the log file transmission configuration

Use the `log host show` CLI command to view whether log file transmission is enabled and which hosts receive log files.

Procedure

1. To display the configuration, enter the `log host show` command.

```
# log host show
Remote logging is enabled.
Remote logging hosts
    log-server
```

Enabling and disabling log message transmission

You must use CLI commands to enable or disable log message transmission.

Procedure

1. To enable sending log messages to other systems, use the `log host enable` command.

2. To disable sending log messages to other systems, use the `log host disable` command.

Adding or removing a receiver host

You must use CLI commands to add or remove a receiver host.

Procedure

1. To add a system to the list that receives protection system log messages, use the `log host add` command.
2. To remove a system from the list that receives system log messages, use the command: `log host del`.

The following command adds the system named *log-server* to the hosts that receive log messages.

```
log host add log-server
```

The following command removes the system named *log-server* from the hosts that receive log messages.

```
log host del log-server
```

The following command disables the sending of logs and clears the list of destination hostnames..

```
log host reset
```

Remote system power management with IPMI

Select DD systems support remote power management using the Intelligent Platform Management Interface (IPMI), and they support remote monitoring of the boot sequence using Serial over LAN (SOL).

IPMI power management takes place between an IPMI initiator and an IPMI remote host. The IPMI initiator is the host that controls power on the remote host. To support remote power management from an initiator, the remote host must be configured with an IPMI username and password. The initiator must provide this username and password when attempting to manage power on a remote host.

IPMI runs independently of DD OS and allows an IPMI user to manage system power as long as the remote system is connected to a power source and a network. An IP network connection is required between an initiator and a remote system. When properly configured and connected, IPMI management eliminates the need to be physically present to power on or power off a remote system.

You can use both DD System Manager and the CLI to configure IPMI users on a remote system. After you configure IPMI on a remote system, you can use IPMI initiator features on another system to log in and manage power.

Note: If a system cannot support IPMI due to hardware or software limitations, DD System Manager displays a notification message when attempting to navigate to a configuration page.

SOL is used to view the boot sequence after a power cycle on a remote system. SOL enables text console data that is normally sent to a serial port or to a directly attached console to be sent over a LAN and displayed by a management host.