تمرین شماره یک : سایت دانشگاه قم 217.218.215.0/26 را با تمام متدهای Scan از طریق Nmap را اجرا کنید و خروجی را در GITHUB بگذارید.

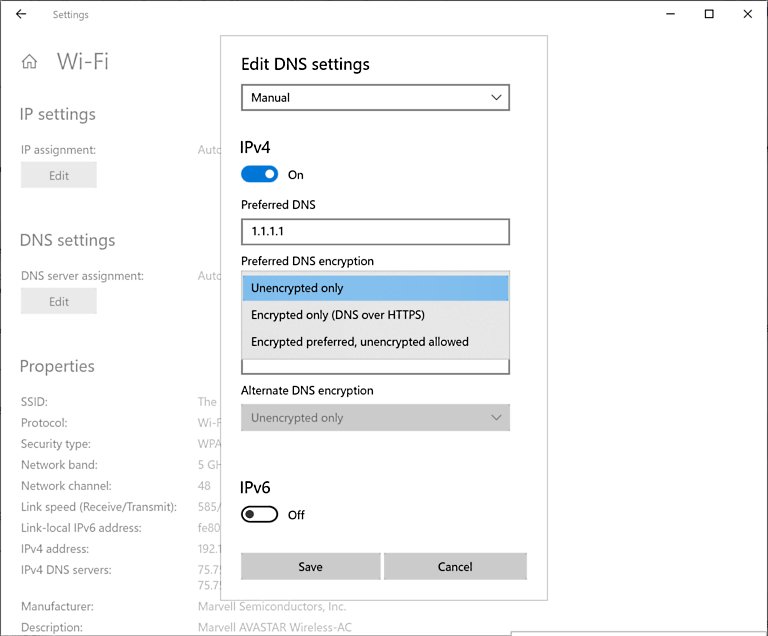




تمرین شماره دو: پروتکل DNS Over HTTPS چیست و چگونه در ویندوز پیاده سازی می شود.

دی او اچ مخفف DNS Over HTTPS بک پروتکل برای انجام رزولوشن (resolution) از راه دور سیستم نام دامنه (DNS) از طریق پروتکل HTTPS است. هدف از این روش افزایش حریم خصوصی و امنیت کاربر از طریق جلوگیری از استراق سمع و دستکاری داده های DNS توسط حملات man-in-the-middle است با استفاده از پروتکل HTTPS برای رمزگذاری داده ها بین DoH Client و DoH-based DNS resolver .

بر اساس شکل ذیل در بخشی که تنظیمات IP سیستم را انجام میدهیم این امکان وجود دارد که مشخص کنیم که ترافیک DNS ما رمزنگاری شده جابجا می شود یا خیر .



تمرین شماره سه : DNS Tunnelling چیست و آنرا پیاده‌سازی کنید. روش شناسائی را شرح دهید.

برای پیاده سازی این حمله کافی است که بتوان IP ، DNS Server قربانی را بتوانیم تغییر دهیم. بر این اساس میتوان IP آدرس وبی که مد نظرمان هست را عوض نموده و قربانی را به سایتی که مدنظرمان هست راهنمایی کنیم.

DNS tunneling با استفاده از درخواست های DNS برای پیاده سازی یک مسیر فرمان و کنترل برای بدافزار استفاده می کند. ترافیک DNS ورودی می تواند دستورات را به بدافزار منتقل کند، در حالی که ترافیک خروجی می تواند داده های حساس را استخراج کند یا به درخواست های اپراتور بدافزار پاسخ دهد. به دلیل اینکه DNS یک پروتکل بسیار انعطاف پذیر است ، می تواند به راحتی مورد حمله تانلینگ قرار گیرد. همچنین محدودیت های بسیار کمی در مورد داده هایی که یک درخواست DNS را شامل می شود وجود دارد زیرا برای جستجوی نام دامنه وب سایت ها طراحی شده است و تقریباً هر چیزی می تواند یک نام دامنه باشد. از فیلدهای نام دامنه می توان برای حمل اطلاعات حساس استفاده کرد. این درخواست‌ها به گونه‌ای طراحی شده‌اند که به سرورهای DNS کنترل‌شده توسط مهاجم بروند و اطمینان حاصل کنند که می‌توانند درخواست‌ها را دریافت کنند و در پاسخ‌های DNS مربوطه پاسخ دهند.

انجام حملات تونل زنی DNS ساده است و مجموعه ابزارهای تونل زنی DNS متعددی وجود دارد. این امکان را برای مهاجمان غیرمجاز نیز فراهم می کند تا از این تکنیک برای پنهان کردن داده ها از راه حل های امنیت شبکه سازمان استفاده کنند.

شناسایی حملات تونل زنی DNS

DNS tunneling شامل سوء استفاده از اساس پروتکل DNS است. بدافزار به جای استفاده از درخواست‌ها و پاسخ‌های DNS برای جستجوی آدرس IP قانونی، از آن برای پیاده‌سازی یک کانال فرمان و کنترل با کنترلر خود استفاده می‌کند.

انعطاف پذیری DNS آن را به انتخاب خوبی برای استخراج داده تبدیل می کند. با این حال، محدودیت های خود را دارد. برخی از شاخص های DNS tunneling در یک شبکه می تواند شامل موارد زیر باشد:

درخواست‌های غیرمعمول دامنه: بدافزار تونل زنی DNS داده‌ها را در یک نام دامنه درخواستی (مانند DATA\_HERE.baddomain.com) رمزگذاری می‌کند. بررسی نام‌های دامنه درخواستی در درخواست‌های DNS ممکن است سازمان را قادر سازد تا ترافیک قانونی را از تلاش برای تونل‌سازی DNS متمایز کند.

درخواست ها برای دامنه‌های غیرمعمول: تونل‌سازی DNS تنها در صورتی کار می‌کند که مهاجم ، مالک دامنه هدف باشد. به طوری که درخواست‌های DNS به سرور DNS آنها برود. اگر سازمانی با افزایش ناگهانی درخواست ها برای یک دامنه غیرمعمول مواجه شود، ممکن است نشان دهنده حمله DNS Tunneling باشد، به خصوص اگر آن دامنه به تازگی ایجاد شده باشد.

حجم بالای ترافیک DNS: نام دامنه در یک درخواست DNS حداکثر اندازه (253 کاراکتر) دارد. بدین معنی که یک مهاجم احتمالاً به تعداد زیادی درخواست DNS مخرب برای استخراج داده یا اجرای یک پروتکل فرمان و کنترل بسیار تعاملی نیاز دارد. جهش حاصل در ترافیک DNS می تواند نشانگر حمله تونل سازی DNS باشد.

هرکدام از عوامل بالا به تنهایی می توانند قابل کنترل باشند. اما ، اگر سازمانی چندین یا همه این ناهنجاری ها را تجربه کند، ممکن است نشانه ای از وجود و فعال بودن بدافزار تونل DNS در شبکه باشد.

تمرین شماره چهار: حملۀ FTP Bounce Back را تشریح کنید.

حمله FTP bounce یک سوء استفاده از پروتکل FTP است که به موجب آن مهاجم می تواند از Command PORT برای درخواست دسترسی به پورت ها به طور غیرمستقیم از طریق استفاده از ماشین قربانی استفاده کند، که به عنوان یک پروکسی برای درخواست عمل می کند. به نوعی مثل یک Mail Relay یا DHCP Relay.

این تکنیک می‌تواند برای اسکن کردن پورت میزبان‌ها به طور محتاطانه، و دور زدن بالقوه لیست کنترل دسترسی شبکه برای دسترسی به پورت‌های خاصی که مهاجم نمی‌تواند از طریق اتصال مستقیم به آنها دسترسی داشته باشد، به عنوان مثال با اسکنر پورت nmap استفاده می‌شود. تقریباً تمام برنامه‌های سرور FTP مدرن به‌طور پیش‌فرض پیکربندی شده‌اند تا Command Port را که به هر میزبانی غیر از میزبان اصلی متصل می‌شوند را رد کنند و حملات bounce FTP را خنثی کنند.

FTP از دو کانال بین کلاینت و سرور استفاده میکند:

* Command channel
* Data channel

این دو کانال از کانکشن های TCP جدا و مستقل از هم استفاده میکنند. Command channel مخصوص دستورات و پاسخ های مربوط به آن ها میباشد و در طرف مقابل Data channel صرفا به منظور انتقال فایل ها مورد استفاده قرار میگیرد. ارسال دستورات به سرور بدون الزام به انتظار برای اتمام انتقال دیتای فعلی، به نظر روشی جذاب میرسد که از طریق استقلال این دو کانال از هم صورت پذیرفته است.در مدل Active، کلاینت برقرار کننده Command channel است (از کلاینت پورت X به سرور پورت 21) و سرور وظیفه ایجاد Data channel را بر عهده دارد (از سرور پورت 20 به کلاینت پورت Y و Y را خود کلاینت تعیین میکند).

تمرین شماره 5 : نصب Cerberud و FileZila و پابلیش بر روی اینترنت

تمرین شماره شش: امن سازی ایمیل :

Exchange:

Mdaemon

Axigent

Postfix

Pound Qube

اساسا برای امن سازی و Hardening هر سرویسی مواردی بصورت عمومی و مواردی دیگر بصورت تخصصی وجود دارد که بطور مثال برای Microsoft Exchange عبارتند از:

* بروزرسانی مداوم سرویس ایمیل
* استفاده از ابزارهای تخصصی برای امنیت بطور مثال:
  + Microsoft Exchange On-Premises Mitigation Tool
  + Microsoft Support Emergency Response Tool
  + Microsoft Security Configuration Wizard

تمرین شماره هفت: حملات ایمیل را تشریح کنید.

چندین نوع حملات در حوزه ایمیل داریم.

فیشینگ : ساخت صفحات جعلی برای دریافت پسورد ایمیل

نفوذ به سیستم : ساخت ویروس و اجرای فایل ویروس توسط قربانی و دسترسی به پسورد های ذخیره شده.

حملات بروت فورس : برای بدست آوردن پسورد با دسترسی مدیریتی

ارسال ایمیل های جعلی و انجام فیشینگ

تمرین شماره هشت: سه تا از Nas Storage های معروف را در اینترنت پیدا کنید.

1 – ASUSTOR

2 – QNAP

3 - Synology

تمرین شماره نه : LOM مربوط به Unitiy 480 را تهیه کنید.

Max Raw Capacity : 4.0 PB

Min/Max Drives: 6/750

Max FAST Cache: Up to 1.2 TBs

Array Enclosure : A 2U Disk Processor Enclosure (DPE) with twenty five 2.5” drives

Drive Enclosure : 2.5" (2U), 25 drives, 2.5" (3U), 80 drives, 3.5" (3U), 15 drives

Memory per Array: 192 GB

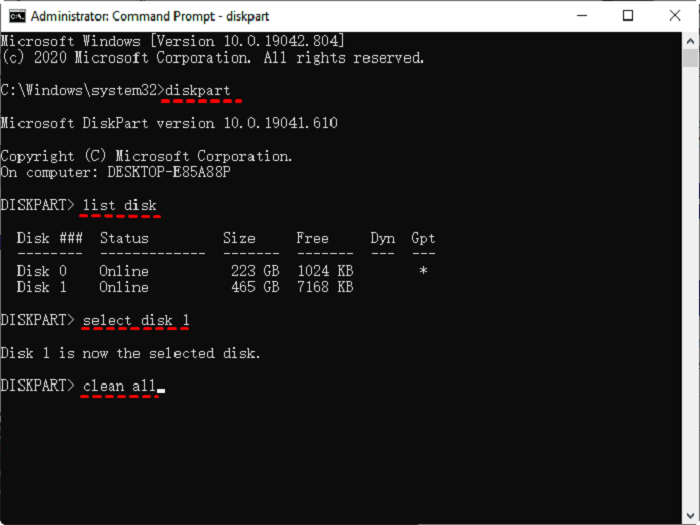
Standby Power System: Dell EMC Unity systems are powered by 2 power supplies (PS) per DPE/DAE. Each power supply can provide power to the entire module if the peer PS has been removed or is faulted. DPE power during a power failure is provided by a Battery Back Up (BBU) module. BBU is located within the SP enclosure and provides power to a single module (power zone).

RAID Options: 1/0, 5, 6

CPU per Array: 2 x dual-socket Intel, CPUs, 32 cores per Array, 1.8GHz

Embedded SAS IO Ports per Array: 4 x 4 lane 12Gb/s SAS, ports for BE Connection.

تمرین شماره ده: هارددیسک یا Flash را Wipe کنید.



تمرین شماره یازده: انواع Raid را بررسی و تشریح کنید.

واژه RAID مخفف اصطلاح Redundant Array of Independent Disks می‌ باشد. کاربرد RAID ایجاد یک کل واحد از مجموع چند هارد دیسک است. به عبارت دیگر با قرار دادن چند هارد دیسک در کنار هم و پیاده سازی RAID همه هارد دیسک ها به یک مجموعه واحد تبدیل شده و سیستم عامل، همه آن ها را به عنوان یک منبع واحد در نظر می گیرد. در تعریف راید به زبان ساده می توان گفت Raid درواقع تکنولوژی مجازی سازی ذخیره دیتا است. برای شناسایی تعداد بسیاری هارد توسط سیستم، باید این هاردها به روشی به هم متصل شوند. این اتصال که به صورت نرم ‌افزاری یا سخت‌ افزاری صورت می‌گیرد، با نام RAID شناخته می‌ شود.

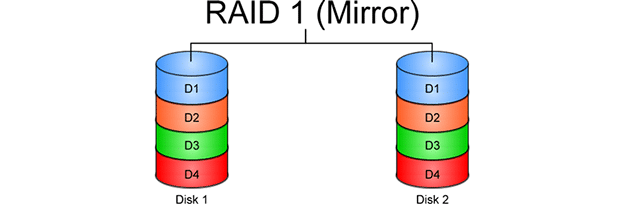
انواع ذخیره سازی در RAID

RAID در واقع آرایه ای است که از دو دیسک سخت و یا بیشتر که در روی یک واحد قرار گرفته اند تشکیل یافته است. برای اینکه به آرایه RAID سه ویژگی بیشتر در مقایسه با JBOD داده شود سه مفهوم اساسی استفاده می شوند.

* Mirroring
* Striping
* Error correction

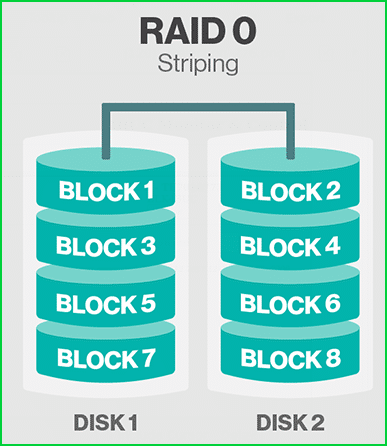
Mirroring

مفهوم Mirroring یعنی داده ها در بیش از یک دیسک نوشته شوند.مثال اساسی Mirroring آرایه RAID1 با دو دیسک می باشد. هر دو دیسک محتوای یکسانی دارند. زمانی که برای درایو اولی مشکلی پیش بیاید، عملیات خواندن و نوشتن به شکل مستقیم در دیسک دوم انجام می شود. عملیات خواندن در ارایه های Mirroring در مقایسه با دیسک تنها به دلیل اینکه سیستم ، داده ها را از چندین دیسک و در یک زمان می خواند سریع تر است. اگرچه عملیات نوشتن از آنجایی که داده ها باید در چند دیسک به جای یک دیسک نوشته شوند، کند تر می باشد. بازسازی آرایه دیسک mirror شده بسیار آسان است داده ها از دیسک سالم به دیسک جدید کپی می شوند . در طول بازسازی کارایی خواندن کاهش پیدا می کند . چرا که تنها یک دیسک mirror قابل استفاده می باشد.



Striping

عملیات جداسازی داده ها از چندین دیسک است.برای مثال آرایه RAID 0 داده ها را در دو دیسک قرار می دهد که این کار تنها کارآیی را افزایش می دهد. عملیات خواندن و نوشتن در آرایه ی Striping در مقایسه با دیسک های تکی سریع تر می باشد.



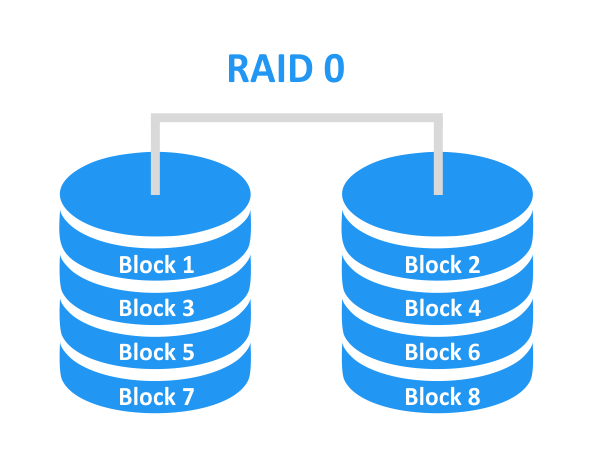
Error correction

داده های parity را با روشی که به آنها اجازه یافته شدن و احتمال تصحیح مشکلات را بدهد بر روی دیسک ذخیره می کند.RAID5 مثال خوبی از مکانیزم تصحیح خطا است .مثلا آرایه RAID5 از سه نوار داده در دو دیسک اول تشکیل یافته و parity را در دیسک سومی قرار می دهد. مکانیزم تصحیح خطا باعث کاهش کارایی خصوصا در عملیات نوشتن می شود چراکه هم داده و هم parity باید نوشته شود. طراحی شمای raid شامل حفاظت از داده و کارایی آن می شود . با توجه به نیازهای سرور شما باید پیکربندی مناسب RAID را انتخاب نمایید .

در ادامه با معرفی هر raid با تفاوت raid ها آشنا می شوید:

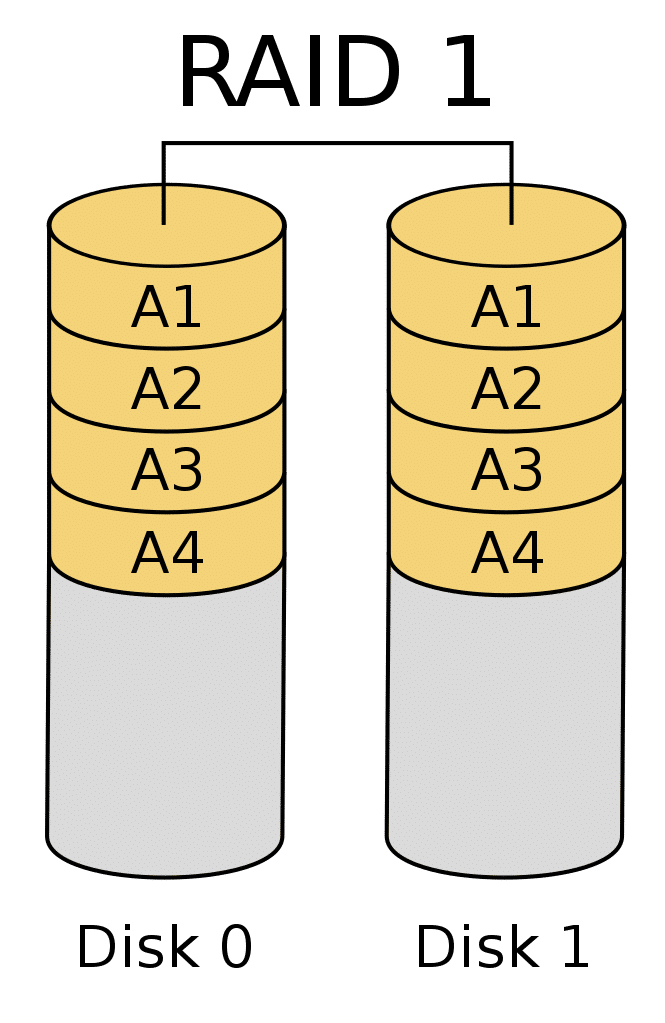
تکنولوژی raid 0 چیست ؟

در تعریف raid و انواع آن ابتدا به بررسی raid 0 می پردازیم، RAID 0 اولین و ساده‌ترین نوع RAID می‌ باشد که به صورت معمول بر روی سیستم‌ عامل ‌ها وجود دارد. در صورتی که در Disk Management سیستم خود دو هارد را با هم به صورت Dynamic و Strip متصل کرده باشید در اصل از این حالت RAID استفاده نموده ‌اید. همانطور که گفته شد دو حالت Stripped و Spanned از انواع RAID 0 می ‌باشد. در این حالت تمام هاردها بدون هیچ هارد رزرو و جایگزین، به صورت متوالی به هم متصل می‌شوند. سرعت در این مدل RAID بسیار بالا می‌باشد و تقریباً از مجموع تمام حجم هاردها می ‌توان استفاده نمود. این مدل RAID باید حداقل دو عدد هارد بر روی سیستم یا Storage وجود داشته باشد.



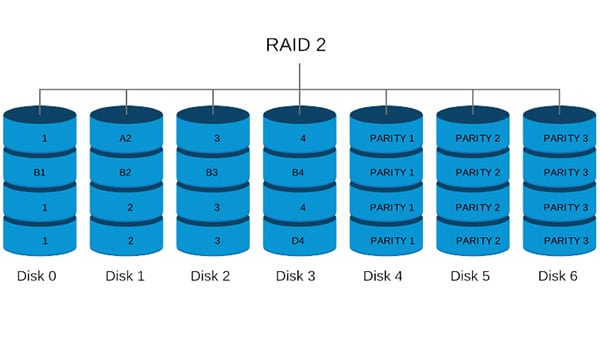
تکنولوژی raid 1

این مدل تقریباً یکی از امن ‌ترین انواع raid در سرورها می ‌باشد. در مدل RAID 1 که حتماً تعداد زوج هارد باید بر روی سیستم یا Storage موجود باشد، نیمی از هاردها به صورت هاردهای رزرو آنلاین برای نیمی دیگر از آنها در نظر گرفته می‌شوند. بدین صورت که در هنگام نوشتن یک فایل بر روی هارد اصلی، یک کپی به عنوان پشتیبان نیز بر روی هارد رزرو نوشته می‌شود. در این حالت سرعت RAID نصف حالت معمول است زیرا عملیات نوشتن دو بار صورت می‌گیرد. اما در صورتی که به هر دلیلی هاردی کامل از بین برود، یک هارد پشتیبان از آن در دستگاه وجود داشته و می‌ توان بدون هیچ مشکل یا قطعی در سیستم، از هارد رزرو استفاده کرد. در مراکز مهم که امنیت بسیار اهمیت بالاتری نسبت به سرعت دارد، از این نوع RAID در انواع هاردهای سیستم‌ ها استفاده می‌شود (دو مدل اول معمولاً بر روی Workstationها اعمال می‌شود و معمولاً در Storageها به دلیل مشکلات موجود استفاده نمی‌شوند).



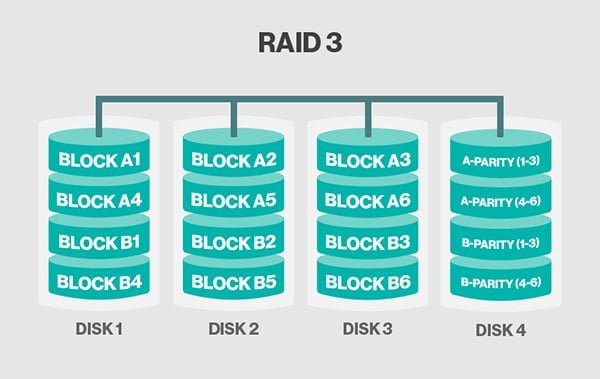
تکنولوژی raid 2

تکنولوژی raid 2 تکنیکی است که از کد Hamming برای تصحیح خطاها استفاده می‌کند Raid 2 از نواربندی در دیسک‌ها و برای تامین امنیت داده از ECC استفاده می‌کند. تکنولوژی RAID 2 به دلیل هزینه بالا و اجرای سخت هم اکنون منسوخ شده است. این رید از نوع ریدهای غیر استاندارد است.



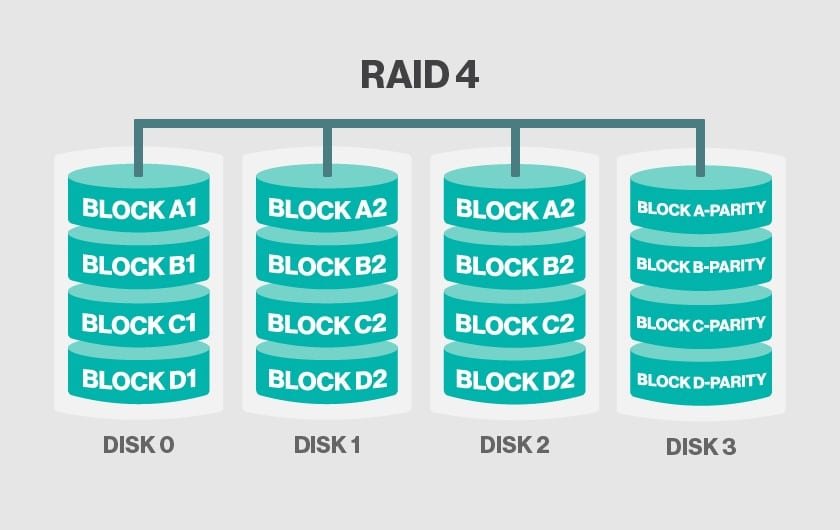
تکنولوژی raid 3

Raid 3 یکی دیگر از انواع raid است که در آن از نواربندی اطلاعات استفاده می‌شود، و یک هارد دیسک را برای ذخیره اطلاعات parity اختصاص داده است. با استفاده از ECC امکان تشخیص خطاها در raid 3 امکان پذیر می‌باشد.



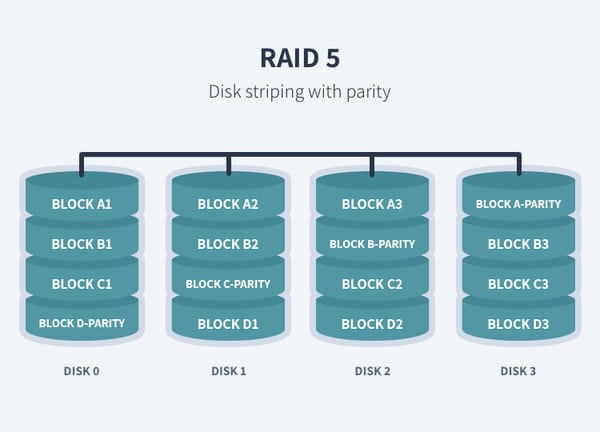
تکنولوژی raid 4

RAID 4 شباهت زیادی به RAID 3 دارد. تفاوت اصلی در نحوه به اشتراک گذاری داده‌ها می‌باشد. این Raid از نوارهای بزرگ استفاده می‌کند. بدین معنی که شما می‌توانید هر رکوردی را از هر درایوی بخوانید. این توزیع به طور چشم‌گیری عملکرد را افزایش می‌دهد. RAID 4 برای پیاده سازی و پیکربندی کامل حداقل به سه دیسک نیاز دارد.



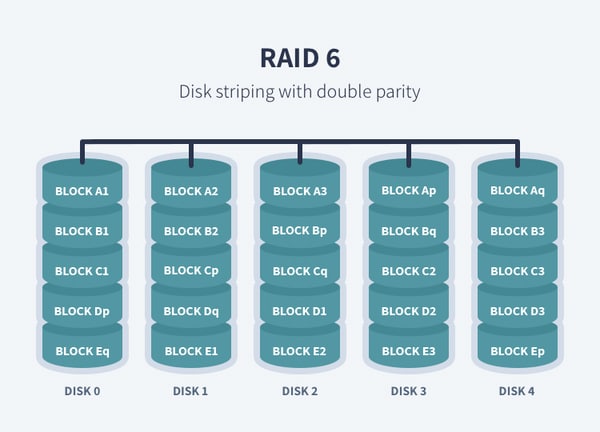
تکنولوژی raid 5 چیست ؟

در مدل RAID 5 حداقل به ۳ دیسک نیاز است. همانند RAID 1 اطلاعات به‌ صورت Mirroring در دیسک‌ ها ذخیره می‌شود. همچنین یک کد parity در بین دیسک‌ ها پخش می‌شود که باعث افزایش کارایی می‌گردد و در هنگام بروز مشکل می‌توان اطلاعات از دست رفته را توسط آن بازیابی کرد. در مقایسه با RAID 1 این سطح ، سرعت کمتری در نوشتن اطلاعات دارد. زیرا زمانی هم برای نوشتن اطلاعات parity مورد نیاز است. در حال حاضر یکی از پرکاربردترین مدل‌ های RAID در انواع Storage ها همین حالت RAID 5 می‌باشد و اکثر قریب به اتفاق Storage ها و برخی از سیستم‌های Workstation خانگی یا اداری از این مدل برای شناسایی تعداد بالای هاردها استفاده می‌کند.



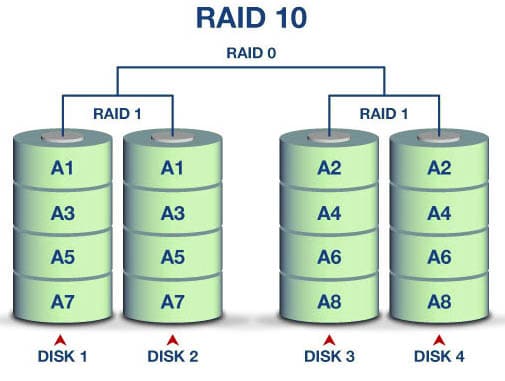
تکنولوژی raid 6

این مدل نیز مانند RAID 5 می‌باشد با این تفاوت که تعداد هارد رزرو آفلاین در مدل RAID 6 به دو عدد افزایش یافته است. این کار باعث افزایش ضریب امنیت در این مدل RAID نسبت به مدل RAID 5 شده است. این مدل از جدیدترین مدل‌های RAID می‌ باشد و به همین خاطر با وجود امنیت و سرعت بالاتر نسبت که RAID 5 ، همچنان تعداد کمتری از Storageها در اقصی نقاط دنیا از این مدل استفاده می‌کنند.



تکنولوژی raid 10

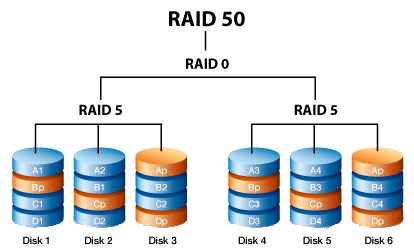
مدل RAID 10 یکی دیگر از انواع RAID می باشد که از ترکیب دو حالت RAID 0 و RAID 1 تشکیل می‌شود. برای مثال در صورتی که ۶ هارد داشته باشیم ، این هاردها با هم RAID 1 شده و امنیت بالایی را به وجود می‌آورند و تعداد ۳ هارد باقیمانده نیز به صورت RAID 0 شده تا سرعت نوشتن بر روی این هاردها نیز به نسبت افزایش یابد (لازم به ذکر است که سرعت در این روش نسبت به حالت RAID 5 , 6 کمتر است).



تکنولوژی raid 50

در مدل RAID 50 نیز از ترکیب دو حالت RAID 0 و RAID 5 استفاده شده است. در برخی از Storageهای معمول ، تنها تعداد محدودی از هارد را می‌توان RAID 5 نمود. این مشکل با معرفی حالت RAID 50 تا حدی برطرف شده است. امروزه در این مدل Storage ها ، در ابتدا تمام هاردها به بخش ‌های کوچک‌ تر تقسیم شده و هر قسمت به صورت RAID 5 تنظیم می‌ شوند. در نهایت تمام بسته‌ های RAID 5 با هم به صورت RAID 0 تنظیم می‌شود تا امکان دسترسی به تمام هاردها و حجم آنها برای کاربران وجود داشته باشد.

لازم به ذکر است در حالت RAID 5 , 6 ، ظرفیت نهایی Storage به دلیل استفاده از هاردهای رزرو و ساختار داخلی این RAIDها پایین می ‌باشد. برای مثال اگر شما Storage با ظرفیت ۲۴ عدد هارد داشته باشید و تمام هاردهای شما نیز ظرفیت ۲ ترابایت داشته باشند ، ظرفیت نهایی در حالت RAID 5 برابر با ۴۰ ترابایت خواهد شد (در حالت معمول باید این مقدار ۴۸ ترابایت باشد).



تمرین شماره دوازده: برندها و Type ها و LOM های مختلف Storage ها را تشریح کنید.

🟦 استوریج اچ پی MSA 2052 SAN Dual Controller SFF

🟦 استوریج اچ پی HPE MSA 2050 SFF

🟦 استوریج HPE MSA 2050 SFF Disk Enclosure

🟦 استوریج HPE MSA 2050 SAN Dual Controller SFF Storage Q1J01B

🟦 استوریج اچ پی MSA 2052 SAN Dual Controller SFF

🟦 MSA 2062 SFF

🟦 SAN 2050 LFF

🟦 SAN 2050 SFF

🟦 SAN 2052 SFF

🟦 2050 LFF Disk Enclosure

🟦 DAS 2050 SFF