مرجع آمـوزش

ویندوز سرور ۲۰۱۶

با پوشش سرفصل‌های دوره

MCSA Windows Server 2016

مؤلف: مهندس اسماعیل یزدانی

انتشارات پندار پارس

سرشناسه : یزدانی، اسماعیل، ۱۳۷۰ -
عنوان و نام پدیدآور : مرجع آموزش ویندوز سرور ۲۰۱۶.../ مولف اسماعیل یزدانی.
مشخصات نشر : تهران : پندار پارس،۱۳۹۶.
مشخصات ظاهری : ۸۰۰ ص.: مصور، جدول.
شابک : 978-600-8201-36-6: ۵۶۰۰۰۰ ریال
وضعیت فهرست نویسی : فیپا
یادداشت : کتابنامه .
موضوع : ویندوز مایکروسافت، سرور
موضوع : Microsoft windows server
موضوع : سیستم‌های عامل (کامپیوتر)
موضوع : Operating systems Computers
رده بندی کنگره : QA۷۶/۷۶ ۱۳۹۶ ۴ی۹۴س/
رده بندی دیویی : ۰۰۵/۴۴۷۶
شماره کتابشناسی ملی : ۴۶۵۸۰۸۹

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ **www.pendarepars.com**

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۲۱۴۳۷۱۹۶۴ **info@pendarepars.com**

ما را در شبکه های اجتماعی دنبال کنید: telegram: @pendarepars

نام کتاب : مرجع آموزش Windows Server 2016، با پوشش سرفصل‌های دوره MCSA WinServer 2016

ناشر : انتشارات پندار پارس

ترجمه و تالیف : اسماعیل یزدانی

چاپ نخست : اردیبهشت ۹۶

شمارگان : ۵۰۰ نسخه

طرح جلد : سارا یعسوبی

چاپ، صحافی : روز

قیمت : ۵۶۰۰۰ تومان **شابک** : ۶-۳۶-۸۲۰۱-۶۰۰-۹۷۸

پیشگفتار:

کتاب حاضر، با نام "مرجع آموزش ویندوز سرور 2016" منبعی جامع و کاربردی درباره نحوه راه‌اندازی، پیکربندی، و مدیریت ویندوز سرور 2016 است که با دو دیدگاه علمی و عملی به بررسی این سیستم‌عامل و سرویس‌های آن پرداخته است.

آموزش‌های کتاب به‌گونه‌ای تنظیم شـده است که بیشتر مباحث دوره MCSA 2016 و در برخی موارد، فراتر از مباحث این دوره را پوشـش می‌دهد. از آنجایی که این مباحث ابتدا از دیدگاه علمی مورد بررسـی و تشـریح قرار می‌گیرد، مخاطب با مطالعه آنها می‌تواند اطلاعات کاملی را در خصـوص مفاهیم و سـرویس‌های ویندوز سـرور کسـب کرده و سـپس با دنبال کردن آموزش‌ها به‌صـورت گام به گام و مصور، نسبت به پیاده‌سازی سرویس‌ها در سناریوهای واقعی اقدام کند.

این کتاب می‌تواند به عنوان منبعی مفید و کامل برای کارشـناسـان و مدیران شـبکه، و همچنین برای افرادی که قصـد دارند در آزمون‌های بین المللی دوره MCSA Windows Server 2016 شـرکت کنند، مورد اسـتفاده قرار گیرد.

امیدوارم با تألیف این کتاب توانسـته باشـم گامی کوچک در راسـتای آموزش علاقه‌مندان به مباحث ویندوز سرور برداشـته باشم. از انجایی که هیچ چیز عاری از نقص و عیب نیست، این کتاب نیز ممکن است دارای کاستی‌هایی باشـد که پیشـاپیش از شما عزیزان پوزش طلبیده و بی‌صبرانه منتظر دریافت نظرات و پیشنهادات شما عزیزان در راستای بهبود مطالب کتاب می‌باشم.

Esmaeil.Yazdani@Ymail.Com

مؤلف: اسماعیل یزدانی

بهار 96

فهرست مطالب

فصل ۱؛ آشنایی با ویندوز سرور ۲۰۱۶ ..... ۱

۱-۱ آشنایی با ویندوز سرور ۲

۱-۲ ویژگی‌ها و تغییرات جدید در ویندوز سرور ۲۰۱۶ ..... ۳

۱-۲-۱ Software-Defined Datacenter ۳

۱-۲-۲ Application Platform ۸

۱-۲-۳ امنیت و مدیریت دسترسی ۱۰

۱-۲-۴ مدیریت سیستم ها ۱۵

فصل ۲؛ نصب و ارتقاء به ویندوز سرور ۲۰۱۶ ..... ۱۷

۲-۱ پیش از نصب ویندوز سرور ۲۰۱۶ ..... ۱۷

۲-۱-۱ برنامه‌ریزی برای نصب ویندوز سرور ۲۰۱۶ ..... ۱۷

۲-۱-۲ آشنایی با ویرایش‌های ویندوز سرور ۲۰۱۶ ..... ۱۸

۲-۱-۳ نیازمندیهای نصب ویندوز سرور ۲۰۱۶ ..... ۱۹

۲-۱-۴ آپشن‌های نصب ویندوز سرور ۲۰۱۶ ..... ۲۰

۲-۲ نصب ویندوز سرور ۲۰۱۶ به صورت Manual ۲۰

۲-۲-۱ نصب ویندوز سرور ۲۰۱۶ با آپشن GUI ۲۱

۲-۲-۲ نصب ویندوز سرور ۲۰۱۶ با آپشن Server Core ۲۷

۲-۳ ارتقاء به ویندوز سرور ۲۰۱۶ ..... ۲۹

۲-۳-۱ ارتقاء ویرایش‌های ویندوز سرور ۲۹

۲-۳-۲ آماده‌سازی برای ارتقاء ۳۰

۲-۳-۳ ارتقاء به ویندوز سرور ۲۰۱۶ ..... ۳۱

فصل ۳؛ پیکربندی مقدماتی سرور ۳۷

۳-۱ پیکربندی ویندوز سرور ۲۰۱۶ ..... ۳۷

۳-۱-۱ اقدامات پیکربندی متداول ۳۷

۳-۱-۲ افزودن سرور به کنسول Server Manager ۴۳

۳-۱-۳ پیکربندی NIC Teaming ۴۶

۳-۲ مدیریت Roleها و Featureها ۴۹

۳-۲-۱ افزودن Roleها و Featureها به سرور ۴۹

۳-۲-۲ نصب Roleها و Featureها برروی دیسک‌های مجازی ۵۴
۳-۲-۳ حذف Roleها و Featureها ۵۶
۳-۳ مهاجرت به ویندوز سرور ۲۰۱۶ ..... ۵۶
۳-۳-۱ آماده‌سازی برای استفاده از Windows Server Migration Tools ۵۷
۳-۳-۲ مهاجرت به کمک Windows Server Migration Tools ۶۲
فصل ۴؛ پیکربندی ذخیره‌سازهای Local ۶۵
۴-۱ برنامه‌ریزی برای فراهم کردن فضای ذخیره‌سازی ۶۵
۴-۱-۱ تعداد سرورهای مورد نیاز ۶۶
۴-۱-۲ محاسبه فضای ذخیره‌سازی ۶۶
۴-۱-۳ استفاده از Storage Spaces ۶۷
۴-۲ آشنایی با تنظیمات دیسک‌ها ۶۸
۴-۲-۱ انتخاب روش پارتیشن‌بندی ۶۸
۴-۲-۲ آشنایی با انوع دیسک‌ها ۶۹
۴-۲-۳ آشنایی با انواع Volumeها ۷۱
۴-۲-۴ آشنایی با File System ۷۲
۴-۳ کار با دیسک‌ها ۷۳
۴-۳-۱ افزودن دیسک‌های فیزیکی به سرور ۷۳
۴-۳-۲ ایجاد و مقداردهی VHD در Computer Management ۷۵
۴-۳-۳ ایجاد Storage Pool ۷۸
۴-۳-۴ ایجاد Virtual Disk در Storage Pool ۸۲
۴-۴ ایجاد و مدیریت Volumeها ۸۷
۴-۴-۱ ایجاد Simple Volume ۸۷
۴-۴-۲ ایجاد Volumeهای Striped، Spanned، Mirrored، RAID-5 ..... ۹۴
فصل ۵؛ مجازی‌سازی به کمک Hyper-V ۹۷
۵-۱ آشنایی با تکنولوژی مجازی‌سازی و ابزار Hyper-V ۹۷
۵-۱-۱ تعریف و انواع روش‌های مجازی‌سازی ۹۷
۵-۱-۲ ویژگیهای جدید Hyper-V در ویندوز سرور ۲۰۱۶ ..... ۹۸
۵-۱-۳ سیستم عامل‌های قابل پشتیبانی در Hyper-V 2016 ..... ۱۰۴
۵-۱-۴ معماری Hyper-V ۱۰۵
۵-۲ نصب و پیکربندی Hyper-V ۱۰۷
۵-۲-۱ نیازمندی‌های نصب Hyper-V ۱۰۷
۵-۲-۲ نصب Hyper-V Role ۱۰۸

۵-۲-۳ بررسی تنظیمات ابزار Hyper-V در کنسول Hyper-V Manager ۱۱۲
۵-۲-۴ تنظیمات Virtual Switches ۱۱۴
۵-۲-۵ ایجاد و مدیریت Virtual Hard disks ۱۱۷
۵-۳ ایجاد و مدیریت Virtual Machines ۱۲۵
۵-۳-۱ ایجاد Virtual Machine ۱۲۶
۵-۳-۲ پیکربندی تنظیمات Virtual Machine ۱۳۱
۵-۳-۳ نصب Integration Components ۱۳۵
۵-۳-۴ Backup و Restore کردن Virtual Machines ۱۳۵
فصل ۶؛ آشنایی با آدرس‌های IP و پیکربندی TCP/IP ۱۳۹
۶-۱ آشنایی با مدل‌های مرجع ۱۳۹
۶-۱-۱ مدل OSI ۱۳۹
۶-۱-۲ مدل TCP/IP ۱۴۴
۶-۲ آشنایی با آدرس‌های IP ۱۴۶
۶-۲-۱ آدرس‌های IPv4 ..... ۱۴۶
۶-۲-۲ کلاس‌های آدرسدهی در IPv4 ..... ۱۴۷
۶-۲-۳ آدرس‌های IPv6 ..... ۱۵۰
۶-۲-۴ انواع آدرس‌های IPv6 ..... ۱۵۱
۶-۳ پیاده‌سازی سابنتینگ در شبکه ۱۵۷
۶-۳-۱ سابنتینگ در IPv4 ..... ۱۵۸
۶-۳-۲ آدرس‌دهی بدون کلاس ۱۷۰
۶-۳-۳ سابنتینگ در IPv6 ..... ۱۷۳
فصل ۷؛ پیکربندی سرویس DNS ۱۷۷
۷-۱ مفاهیم پایه DNS ۱۷۷
۷-۲ نصب و پیکربندی سرویس DNS ۱۸۰
۷-۲-۱ نصب DNS Server ۱۸۰
۷-۲-۲ آشنایی با انواع Zoneها ۱۸۲
۷-۲-۳ ایجاد و مدیریت Zoneها ۱۸۴
۷-۲-۴ یکپارچگی با سایر سرورهای DNS ۱۹۶
۷-۳ ایجاد و مدیریت رکوردها در DNS ۲۰۱
فصل ۸؛ پیکربندی سرویس DHCP ۲۱۳
۸-۱ آشنایی با مفاهیم و پردازش‌های اساسی در سرویس DHCP ۲۱۳

۸-۱-۱ معرفی پردازش DORA ۲۱۳
۸-۱-۲ مزایا و معایب سرویس DHCP ۲۱۵
۸-۱-۳ DHCP Lease ۲۱۶
۸-۱-۴ DHCP Lease Renewal ۲۱۸
۸-۱-۵ آزادسازی DHCP Lease ۲۱۸
۸-۱-۶ آشنایی با Scopeهای DHCP ۲۱۸
۸-۲ نصب و راه اندازی سرویس DHCP ۲۲۰
۸-۲-۱ نصب سرویس DHCP ۲۲۰
۸-۳ ایجاد و مدیریت Scopeها در DHCP ۲۲۴
۸-۳-۱ ایجاد Scope در IPv4 ..... ۲۲۴
۸-۳-۲ ایجاد Scope در IPv6 ..... ۲۳۰
۸-۳-۳ تغییر تنظیمات Scope (IPv4 و IPv6) ۲۳۲
۸-۳-۴ مدیریت Reservation و Exclusion ۲۳۵
۸-۳-۵ تنظیمات Scope Options در IPv4 ..... ۲۳۷
۸-۳-۶ ایجاد و حذف Superscope در IPv4 ..... ۲۳۹
۸-۳-۷ ایجاد Multicast Scope در IPv4 ..... ۲۴۱
۸-۴ مانیتورینگ و نگهداری از DHCP ۲۴۴
۸-۴-۱ یکپارچه‌سازی DDNS با DHCP ۲۴۴
۸-۴-۲ نظارت بر Leaseهای DHCP ۲۴۵
۸-۴-۳ ثبت فعالیت‌های DHCP ۲۴۶
۸-۴-۴ کار با پایگاه داده DHCP ۲۴۷
فصل ۹؛ سرویس‌های دامنه در Active Directory ۲۴۹
۹-۱ آشنایی با مفاهیم پایه اکتیو دایرکتوری ۲۴۹
۹-۲ ایجاد جنگل تک دامنه‌ای و افزودن Domain Controller به آن ۲۵۴
۹-۲-۱ ایجاد جنگل تک دامنه‌ای ۲۵۵
۹-۲-۲ افزودن Domain Controller به جنگل ۲۶۲
۹-۳ ایجاد و مدیریت Accounts، Groups و Organizational Units ۲۶۵
۹-۳-۱ ایجاد و مدیریت اشیاء به کمک Active Directory Users and Computers ... ۲۶۵
۹-۳-۲ ایجاد و مدیریت اشیاء به کمک Active Directory Administrative Center . ۲۷۵
۹-۳-۳ تعیین سطح دسترسی (حقوق) کاربران و گروه‌ها در اکتیو دایرکتوری ۲۷۹
۹-۴ اقدامات مرتبط با مدیریت اکتیو دایرکتوری ۲۸۲
۹-۴-۱ پیوستن سرور به یک دامنه ۲۸۲

۹-۴-۲ حذف کردن DC و انهدام آن ۲۸۳
۹-۴-۳ افزایش سطح عملکرد دامنه و جنگل ۲۸۶
۹-۴-۴ بازیابی رمز عبور Administrator ۲۸۷
۹-۴-۵ تغییر نام دامنه ۲۸۸
فصل ۱۰؛ پیکربندی تنظیمات Group Policy ۲۹۱
۱۰-۱ مدیریت و نگهداری از Group Policy Objects ۲۹۱
۱۰-۱-۱ ایجاد و مدیریت GPO ۲۹۲
۱۰-۱-۲ واگذاری مجوز برای ویرایش GPO ۲۹۴
۱۰-۱-۳ Backup، Restore، Import و Copy کردن GPOها ۲۹۵
۱۰-۲ مدیریت عملکردهای Group Policy ۲۹۸
۱۰-۲-۱ اولویت پردازش Policy ۲۹۹
۱۰-۲-۲ اجرا و مسدود کردن Policy ۳۰۰
۱۰-۲-۳ فیلترهای امنیتی در Group Policy ۳۰۱
۱۰-۲-۴ فیلترهای WMI ۳۰۳
۱۰-۲-۵ Loopback Processing ۳۰۵
۱۰-۲-۶ Group Policy برروی لینک‌های کم سرعت ۳۰۷
۱۰-۳ تنظیمات پایه Group Policy ۳۰۸
۱۰-۳-۱ Folder Redirection ۳۰۸
۱۰-۳-۲ نصب نرم افزارها به کمک Group Policy ۳۱۱
۱۰-۳-۳ استفاده از اسکریپت‌ها در Group Policy ۳۱۴
۱۰-۴ الگوهای Administrative Templates ۳۱۶
۱۰-۴-۱ تنظیمات Administrative Templates ۳۱۶
۱۰-۴-۲ Central Store ۳۱۹
۱۰-۴-۳ فیلتر کردن Policyها بر اساس تنظیمات ۳۲۱
۱۰-۵ مدیریت Group Policy Preferences ۳۲۲
۱۰-۵-۱ نگاشت Network Drives ۳۲۲
۱۰-۵-۲ پیکربندی و نگاشت پرینترها ۳۲۴
۱۰-۵-۳ پیکربندی تنظیمات Power ۳۲۶
۱۰-۵-۴ تنظیمات اینترنت ۳۲۹
فصل ۱۱؛ پیکربندی سرویس‌های فایل و ایجاد File Server ۳۳۱
۱۱-۱ پیکربندی سرویس File Server Resource Manager ۳۳۱
۱۱-۱-۱ نصب سرویس File Server Resource Manager ۳۳۲

۱۱-۱-۲ ایجاد و مدیریت Quota ۳۳۳
۱۱-۱-۳ ایجاد و مدیریت File Screens ۳۳۷
۱۱-۱-۴ مدیریت گزارش‌های مرتبط با ذخیره‌سازی ۳۴۰
۱۱-۲ پیکربندی سیستم فایل توزیع شده (DFS) ۳۴۳
۱۱-۲-۱ DFS Namespaces ۳۴۴
۱۱-۲-۲ DFS Replication ۳۴۷
۱۱-۳ اشتراک گذاری فایل‌ها و پوشه‌ها و اختصاص مجوزهای دسترسی ۳۵۴
۱۱-۳-۱ اشتراک گذاری و اختصاص مجوزها به کمک Server Manager ۳۵۴
۱۱-۳-۲ اشتراک گذاری و اختصاص مجوزها به کمک Windows Explorer ۳۶۳
۱۱-۴ پیکربندی Data Deduplication ۳۶۵
۱۱-۴-۱ نحوه عملکرد سرویس Data Deduplication ۳۶۵
۱۱-۴-۲ نصب سرویس Data Deduplication ۳۶۶
۱۱-۴-۲ پیکربندی سرویس Data Deduplication ۳۶۶
۱۱-۵ پیکربندی سرویس BranchCache ۳۶۸
۱۱-۵-۱ نصب و فعال‌سازی سرویس BranchCache برروی Content Server ۳۶۹
۱۱-۵-۱ پیاده‌سازی BranchCache به روش توزیع شده ۳۷۱
۱۱-۵-۲ پیاده‌سازی BranchCache به روش میزبانی شده ۳۷۴
فصل ۱۲؛ پیکربندی سرویس چاپ و ایجاد Print Server ۳۸۱
۱۲-۱ آشنایی با اجزاء و ساختار سیستم Print ۳۸۱
۱۲-۱-۱ آشنایی با اجزاء سرویس Print ۳۸۱
۱۲-۱-۲ آشنایی با سیستم Print در ویندوز ۳۸۲
۱۲-۱-۳ معماری‌های سیستم Print ۳۸۳
۱۲-۲ افزودن و اشتراک گذاری پرینتر در شبکه ۳۸۵
۱۲-۲-۱ افزودن پرینتر به شبکه ۳۸۶
۱۲-۲-۲ اشتراک گذاری پرینتر در شبکه ۳۸۹
۱۲-۳ نصب و راه اندازی Print Server ۳۹۱
۱۲-۳-۱ نصب Print and Document Services ۳۹۱
۱۲-۳-۲ آشنایی با کنسول Print Management ۳۹۳
۱۲-۳-۳ مدیریت پرینترها در کنسول PMC ۳۹۶
۱۲-۳-۴ استقرار پرینتر به کمک Group Policy ۴۰۵
فصل ۱۳؛ مدیریت زیرساخت IP به کمک IPAM Server ۴۰۷
۱۳-۱ آشنایی با IPAM و قابلیت‌های آن ۴۰۷

۱۳-۱-۱ قابلیت‌های IPAM ۴۰۸
۱۳-۱-۲ توپولوژی‌های پیاده‌سازی IPAM ۴۱۱
۱۳-۱-۳ معماری IPAM ۴۱۲
۱۳-۲ نصب و راه اندازی IPAM ۴۱۷
۱۳-۲-۱ نیازمندی‌های نرم افزاری و سخت افزاری نصب IPAM ۴۱۷
۱۳-۲-۲ نکات و الزامات نصب IPAM ۴۱۸
۱۳-۲-۳ نصب IPAM ۴۱۹
۱۳-۲-۴ راه اندازی و پیکربندی IPAM Server ۴۲۰
فصل ۱۴؛ استقرار Imageها به کمک MDT و WDS ۴۳۱
۱۴-۱ استقرار سیستم عامل به کمک ابزارهای WADK (ADK) و MDT ۴۳۱
۱۴-۱-۱ روش‌های پیاده‌سازی استقرار به کمک MDT ۴۳۱
۱۴-۱-۲ دانلود و نصب ابزار WADK (ADK) ۴۳۲
۱۴-۱-۳ دانلود و نصب ابزار MDT ۴۳۵
۱۴-۱-۴ استقرار سیستم عامل و نرم افزارها به کمک MDT ۴۳۸
۱۴-۲ استقرار سیستم عامل به کمک سرویس WDS ۴۵۸
۱۴-۲-۱ نصب سرویس WDS ۴۵۹
۱۴-۲-۲ پیکربندی سرور WDS ۴۶۱
۱۴-۲-۳ افزودن Image به سرویس WDS ۴۶۴
۱۴-۲-۴ استقرار ویندوز ۱۰ به کمک سرویس WDS ۴۶۸
فصل ۱۵؛ مدیریت آپدیت‌ها به کمک سرویس WSUS ۴۷۱
۱۵-۱ فازهای مدیریت آپدیت (Update/Path Management) ۴۷۱
۱۵-۱-۱ فاز اول: Assess (ارزیابی) ۴۷۲
۱۵-۱-۲ فاز دوم: Identity (شناسایی) ۴۷۲
۱۵-۱-۳ فاز سوم: Evaluate and Plan (ارزیابی و طرح‌ریزی) ۴۷۳
۱۵-۱-۴ فاز چهارم: Deploy (استقرار) ۴۷۳
۱۵-۲ نصب و پیکربندی Windows Server Update Service (WSUS) ۴۷۴
۱۵-۲-۱ برنامه‌ریزی برای استقرار WSUS ۴۷۴
۱۵-۲-۲ نصب و راه اندازی سرویس WSUS ۴۷۷
۱۵-۲-۳ پیکربندی WSUS ۴۸۰
۱۵-۲-۴ تنظیمات فایروال برای دسترسی سرورهای WSUS ۴۸۷
۱۵-۲-۵ پیکربندی تنظیمات برای دریافت آپدیت‌ها توسط کاربران ۴۸۸
فصل ۱۶؛ ایجاد و مدیریت گواهینامه‌ها به کمک سرویس AD CS ۴۹۳

۱۶-۱ معرفی سرویس Active Directory Certificate Services ۴۹۳
۱۶-۱-۱ آشنایی با زیرساخت کلید عمومی (PKI) ۴۹۳
۱۶-۱-۲ انواع گواهینامه-ها و موارد استفاده از آنها ۴۹۷
۱۶-۲ نصب و راه اندازی سرویس AD CS ۴۹۸
۱۶-۲-۱ نصب AD CS – ایجاد و پیکربندی Certification Authority (CA) ۴۹۸
۱۶-۲-۲ نصب و پیکربندی Certification Authority Web Enrollment ۵۰۹
۱۶-۲-۳ نحوه ایجاد گواهینامه – گواهینامه SSL (HTTPS) ۵۱۲
۱۶-۲-۴ نصب و پیکربندی سرویس‌های Certificate Enrollment Web Service و
Certificate Enrollment Policy Web Service ۵۲۱
۱۶-۲-۵ نصب و پیکربندی Network Device Enrollment Service ۵۲۷
۱۶-۲-۶ نصب و پیکربندی Online Responder ۵۳۰
۱۶-۳ مدیریت سرور CA و سرویس‌های AD CS ۵۳۳
۱۶-۳-۱ مهاجرت CA از یک سرور به دیگری ۵۳۳
۱۶-۳-۲ اقدامات مرتبط با ایجاد و مدیریت گواهینامه‌ها ۵۳۴
فصل ۱۷؛ پیکربندی سرویس‌های Remote Access ۵۳۹
۱۷-۱ نصب و پیکربندی سرویس VPN ۵۳۹
۱۷-۱-۱ آشنایی با VPN ۵۳۹
۱۷-۱-۲ آشنایی با پروتکل‌های Tunneling در VPN ۵۴۱
۱۷-۱-۳ نصب Remote Access role ۵۴۲
۱۷-۱-۴ پیکربندی Routing and Remote Access (سرویس VPN) ۵۴۶
۱۷-۱-۵ افزودن Policyهای مورد نیاز به کمک NPS ۵۵۰
۱۷-۱-۶ محدود کردن آدرسهای IP به کمک IP Filters ۵۵۷
۱۷-۱-۷ افزودن گواهینامه SSL به سرور VPN (پیکربندی SSTP VPN) ۵۵۸
۱۷-۱-۸ تنظیمات Firewall ۵۶۰
۱۷-۱-۹ ایجاد کانکشن VPN و اتصال کاربران به سرور ۵۶۰
۱۷-۱-۱۰ امن‌سازی ارتباطات VPN به کمک IPsec ۵۶۵
۱۷-۲ نصب و پیکربندی سرویس DirectAccess ۵۷۲
۱۷-۲-۱ نصب سرویس DirectAccess ۵۷۲
۱۷-۲-۲ پیکربندی سرویس DirectAccess ۵۷۳
۱۷-۳ نصب و پیکربندی سرویس NAT ۵۸۲
۱۷-۳-۱ آشنایی با NAT ۵۸۲
۱۷-۳-۲ نصب سرویس NAT (سرویس Routing) ۵۸۳

۱۷-۳-۳ پیکربندی سرویس NAT ۵۸۳
۱۷-۴ نصب و پیکربندی سرویس Routing ۵۸۶
۱۷-۴-۱ آشنایی با مفهوم مسیریابی ۵۸۶
۱۷-۴-۲ نصب و پیکربندی سرویس Routing ۵۸۷
۱۷-۴-۳ پیکربندی Static Route ۵۸۷
۱۷-۴-۴ پیکربندی RIP ۵۸۸
۱۷-۴-۵ پیکربندی IGMP ۵۹۱
فصل ۱۸؛ ایجاد محیط‌های گسترده در Active Directory ۵۹۳
۱۸-۱ افزودن جنگل و دامنه‌های اضافه به اکتیو دایرکتوری ۵۹۳
۱۸-۱-۱ افزودن جنگل‌های اضافه به اکتیو دایرکتوری ۵۹۳
۱۸-۱-۲ افزودن دامنه‌های اضافه به جنگل‌ها ۵۹۵
۱۸-۲ پیکربندی سایت‌ها در اکتیو دایرکتوری ۵۹۹
۱۸-۲-۱ ایجاد سایت ۵۹۹
۱۸-۲-۲ ایجاد Subnet ۶۰۱
۱۸-۲-۳ افزودن و انتقال سرور DC به سایت ۶۰۲
۱۸-۲-۴ ایجاد Site Link و تنظیمات Replication ۶۰۲
۱۸-۳ ایجاد و مدیریت Trust میان دامنه‌ها و جنگل‌ها در اکتیو دایرکتوری ۶۰۴
۱۸-۵-۱ مفاهیم Trust ۶۰۴
۱۸-۵-۲ انواع Trust ۶۰۶
۱۸-۵-۳ ایجاد Trust ۶۰۸
۱۸-۴ نصب و پیکربندی Read Only Domain Controllers (RODC) ۶۱۶
۱۸-۴-۱ سیاست‌های مرتبط با تکثیر Passwordها در RODC ۶۱۷
۱۸-۴-۲ نصب و پیاده‌سازی RODC ۶۱۸
۱۸-۵ بررسی و پیکربندی FSMO roles (Operations Master roles) ۶۲۱
۱۸-۵-۱ روش‌های Multi-master و Single-master برای تکثیر آپدیت‌ها ۶۲۲
۱۸-۵-۲ Schema master ۶۲۲
۱۸-۵-۳ Domain naming master ۶۲۲
۱۸-۵-۴ Relative identifier (RID) master ۶۲۲
۱۸-۵-۵ PDC emulator master ۶۲۳
۱۸-۵-۶ Infrastructure master ۶۲۳
۱۸-۵-۷ انتقال FSMO Roles میان سرورهای DC ۶۲۴
فصل ۱۹؛ پیکربندی سرویس‌های Remote Desktop ۶۳۱

۱۹-۱ آشنایی با Remote Desktop Services ۶۳۱
۱۹-۱-۱ دلایل استفاده از سرویس‌های Remote Desktop ۶۳۲
۱۹-۱-۲ آشنایی با مدل پردازش Remote Desktop Services ۶۳۲
۱۹-۲ نصب و پیکربندی Remote Desktop Services role ۶۳۴
۱۹-۲-۱ نصب و پیکربندی Remote Desktop Services (RDSH، RDCB، RDWA) ۶۳۶
۱۹-۲-۲ نصب و پیکربندی Remote Desktop Licensing (RDL) ۶۴۴
۱۹-۲-۳ نصب و پیکربندی Remote Desktop Gateway (RDG) ۶۵۷
۱۹-۲-۴ نصب و پیکربندی Remote Desktop Virtualization Host (RDVH)..... ۶۶۷
فصل ۲۰؛ Backup گیری از سرورها و اکتیو دایرکتوری ۶۸۱
۲۰-۱ ابزارهای ایجاد Backup در ویندوز سرور ۶۸۱
۲۰-۱-۱ Windows Server Backup ۶۸۲
۲۰-۱-۲ Volume Shadow Copy Service (VSS) ۶۸۳
۲۰-۲ Backup گیری و بازگردانی محتویات سرور ۶۸۴
۲۰-۲-۱ ایجاد Backup از سرور به روش زمان‌بندی شده ۶۸۵
۲۰-۲-۲ ایجاد Backup از سرور به روش Manual ۶۸۹
۲۰-۲-۲ بازگردانی محتویات Backup گیری شده ۶۹۲
۲۰-۳ Backupگیری و بازگردانی اکتیو دایرکتوری ۶۹۶
۲۰-۳-۱ Backupگیری از اکتیو دایرکتوری ۶۹۶
۲۰-۳-۲ بازگردانی اکتیو دایرکتوری به روش Non-Authoritative ۶۹۷
۲۰-۳-۲ بازگردانی اکتیو دایرکتوری به روش Authoritative ۷۰۱
۲۰-۳-۲ بازگردانی اشیاء اکتیو دایرکتوری به کمک Active Directory Recycle Bin ۷۰۲
فصل ۲۱؛ آشنایی با Server Core و پیکربندی سرور در خط فرمان ۷۰۵
۲۱-۱ آشنایی با Server Core و نصب و پیکربندی آن ۷۰۵
۲۱-۱-۱ نصب Server Core ۷۰۶
۲۱-۱-۲ راهنمایی‌های ضروری در Server Core ۷۰۷
۲۱-۲ پیکربندی مقدماتی سرور به کمک Sconfig، Cmd، و PowerShell ۷۰۹
۲۱-۲-۱ پیکربندی مقدماتی سرور به کمک ابزار Sconfig ۷۰۹
۲۱-۲-۲ پیکربندی مقدماتی سرور به کمک دستورات Cmd ۷۱۱
۲۱-۲-۳ پیکربندی مقدماتی سرور به کمک PowerShell ۷۱۳
۲۱-۳ پیکربندی Roleها، Featureها، و سرویس‌ها به کمک خط فرمان ۷۱۸
۲۱-۳-۱ سرویس‌های قابل پشتیبانی در Cmd ۷۱۸
۲۱-۳-۲ نصب و پیکربندی Active Directory ۷۱۹

۲۱-۳-۳ نصب و پیکربندی سرویس DNS ۷۲۶
۲۱-۳-۴ نصب و پیکربندی سرویس DHCP ۷۲۸
۲۱-۳-۵ نصب و پیکربندی File Server ۷۲۹
۲۱-۳-۶ نصب و پیکربندی Backup Server ۷۳۱
۲۱-۴ پیکربندی Roleها، Featureها، و سرویس‌ها به کمک PowerShell ۷۳۲
۲۱-۴-۱ سرویس‌های قابل پشتیبانی در PowerShell ۷۳۲
۲۱-۴-۲ نصب و پیکربندی Active Directory ۷۳۳
۲۱-۴-۳ نصب و پیکربندی سرویس DNS ۷۳۵
۲۱-۴-۴ نصب و پیکربندی سرویس DHCP ۷۳۷
۲۱-۴-۵ نصب و پیکربندی File Server ۷۳۷
فصل ۲۲: پیکربندی و مدیریت Nano Server ۷۳۹
۲۲-۱ آشنایی با Nano Server ۷۳۹
۲۲-۱-۱ مقایسه Nano Server با سایر ویرایش‌های ویندوز سرور ۷۳۹
۲۲-۱-۲ دسترسی به Nano Server ۷۴۰
۲۲-۲ نصب و راه اندازی Nano Server ۷۴۰
۲۲-۲-۱ پیاده‌سازی سریع Nano Server ۷۴۱
۲۲-۲-۲ پیاده‌سازی Nano Server به کمک ابزار Nano Server Image Builder ۷۴۴
۲۲-۲-۳ ایجاد Imageهای سفارشی از Nano Server (در PowerShell) ۷۵۴
۲۲-۲-۴ بررسی محیط Nano Server Recovery Console ۷۵۹
۲۲-۳ نصب Roleها و Featureها در Nano Server ۷۶۴
۲۲-۳-۱ جستجو و نصب Providerهای مربوط به Packageها ۷۶۴
۲۲-۳-۲ جستجو، دریافت، و نصب Packageها ۷۶۴
۲۲-۳-۳ نصب Roleها و Featureها به صورت Local ۷۶۸
۲۲-۴ سایر اقدامات مرتبط با ایجاد و ویرایش Nano Server image ۷۶۹
۲۲-۴-۱ اتصال به دامنه ۷۶۹
۲۲-۴-۲ نصب درایورهای اضافه ۷۶۹
۲۲-۴-۳ تزریق درایورها ۷۷۱
۲۲-۴-۴ فعال‌سازی قابلیت اتصال از طریق WinRM ۷۷۱
۲۲-۴-۵ تنظیم آدرس IP به صورت Static ۷۷۱
۲۲-۴-۶ تغییر حجم فایل Image ۷۷۱
۲۲-۵ مدیریت و نگهداری از Nano Server ۷۷۲
۲۲-۵-۱ اتصال به Nano Server ۷۷۲

۲-۵-۲۲ نگهداری از Nano Server ۷۷۴

فصل ۱

آشنایی با ویندوز سرور ۲۰۱۶

در دنیای کنونی، فناوری اطلاعات و ارتباطات از جایگاه ویژه‌ای برخوردار اســت به گونه‌ای که کمتر ســازمان یا کسب و کاری را خواهید یافت که فناوری اطلاعات نقشی در پیشبرد اهداف آنها نداشته باشد. گسترش روز افزون ارتباطات و به‌ویژه شبکه های کامپیوتری، سازمان‌ها و شرکت‌های کوچک و بزرگ را وادار کرده است تا به منظور اجرای هرچه بهتر امورات خود از سیستم‌ها و تکنولوژی‌های ارائه شده در این زمینه بهره گیرند.

اکثر امورات روزمره انسـان‌ها مانند چک کردن ایمیل‌ها و اکانت‌ها در شـبکه‌های اجتماعی، خرید اینترنتی، واریز و برداشت وجه از حساب‌های بانکی و ... همگی بر اساس ساختارهای ارئه شده توسط شبکه‌های کامپیوتری در حال انجام هسـتند. شـبکه‌های بزرگی همچون اینترنت، متشـکل از تعداد زیادی کامپیوتر مرکزی (سـرور) هسـتند که وظیفه دریافت و پردازش درخواسـت‌های مرتبط با کاربران در سـرتاسـر دنیا را برعهده دارند. شـبکه‌های کوچکتر (کارخانجات، سـازمان‌ها، شـرکت‌ها و ...) نیز از این قاعده مستثنی نبوده و باید برای پاسخگویی به درخواست‌های کاربران خود از این کامپیوترهای سرویس‌دهنده استفاده کنند. اما چه قابلیت‌های منحصر به‌فردی در سرورها وجود دارد که آنها را به مهره‌ای کلیدی در ساختار شبکه‌ها تبدیل کرده است ؟ اجازه دهید با یک مثال آنرا شرح دهیم.

فرض کنید یک شـبکه متشـکل از ۱۰ یا حداکثر ۲۰ کاربر با حجم کمی از درخواسـت‌ها و ترافیک‌های ارسـالی برروی شـبکه می‌باشـد. در این شـبکه به دلیل وجود بار پردازشـی کم می‌توان از کامپیوترهای معمولی (در قالب سـاختار Workgroup) به منظور دریافت و پردازش این درخواسـت ها اسـتفاده کرد و بنابراین مدیریت آنها کار چندان دشـواری نخواهد بود. اما زمانی که تعداد کاربران شـبکه افزایش پیدا می کند (به عنوان مثال شـبکه‌ای با ۵۰۰۰ کاربر را در نظر بگیرید) و قرار اسـت این کاربران بطور همزمان به منابع مشـترکی مثل پایگاه‌داده، فایل‌ها، برنامه‌های کاربری، پرینتر و ... دسـترسـی داشته باشند مدیریت درخواست‌ها، پردازش‌ها، اولویت استفاده از پرینتر، برقراری امنیت، احراز هویت کاربران و مسائلی از این قبیل می‌تواند به مسئله‌ای جدی تبدیل شود که از عهده یک شـبکه Workgroup خارج اسـت. در اینجا اسـت که نقش سـرویس دهنده هایی مرکزی (سرورها) که قادر به پاسـخگویی به این نیازها باشـند پررنگ تر گشـته و مدیران شبکه ملزم می‌شوند از آنها به عنوان بخش مهمی از ساختار شبکه خود استفاده کنند.

سرورها برای پاسخگویی به درخواست‌های کاربران باید از سیستم‌عامل مناسبی برخوردار باشند. سیستم‌عامل‌هایی مانند لینوکس[1]، یونیکس[2] و ویندوز سـرور[3]، نمونه‌های مشـهوری در این زمینه می‌باشند. در این کتاب قصد داریم

[1] Linux
[2] Unix
[3] Windows Server

به بررسی ویندوز سرور ۲۰۱۶ پرداخته و شما را با سرویس‌های مهم و کاربردی آن آشنا کنیم. از آنجایی که در ورژن ۲۰۱۶ تغییرات بسیاری در سیستم عامل ویندوز سرور لحاظ شده است، فصل اول از کتاب را به معرفی این سیستم عامل و تغییرات ایجاد شده در آن اختصاص می دهیم. به‌طور کلی مهمترین مباحث ارائه شده در این فصل عبارتند از:

- آشنایی با ویندوز سرور
- معرفی ویژگی‌ها و تغییرات جدید در Windows Server 2016

۱-۱آشنایی با ویندوز سرور

شرکت مایکروسافت در بازه زمانی ۳ تا ۵ سال ورژن جدیدی از سیستم عامل‌های خود را به بازار عرضه می‌کند. این سیستم عامل‌ها در دو گروه Client و Server جای گرفته و هرکدام به‌نحوی نیاز سازمان‌ها برای پیشبرد اهداف IT را برطرف می‌نمایند. در حال حاضر جدیدترین سیستم عامل‌های مایکروسافتی ارائه شده به بازار، Windows Server 2016 (سمت سرور[1]) و Windows 10 (سمت کلاینت[2]) می‌باشند.

Windows Server نام تجاری گروهی از سیستم عامل‌های سرور است که نخستین ورژن آن تحت عنوان Windows Server 2003 به بازار ارائه گردید. تا قبل از انتشار این سیستم عامل، سیستم عامل‌های قدیمی‌تر همچون Windows NT 3.1 Advanced Server، Windows NT 3.5 Server، Windows NT 4.0 Server و در نهایت Windows 2000 Server خدمات مرتبط با سرور را در اختیار کاربران شبکه قرار می‌دادند. Windows 2000 Server، نخستین سیستم عامل مایکروسافت است که از سرویس‌هایی همچون Active Directory، DNS Server، DHCP Server، Group Policy و بسیاری از سرویس‌های دیگری که امروزه مورد استفاده قرار می‌گیرند بهره‌مند گردید.

خانواده Windows Server از ورژن ۲۰۰۳ شروع شده و (تا زمان نگارش این کتاب) به ورژن ۲۰۱۶ منتهی می‌شود. در جدول زیر، فهرست ورژن‌های مختلف این خانواده و زمان انتشار آنها نمایش داده شده است.

جدول ۱-۱: فهرست ورژن‌های مختلف ویندوز سرور و زمان انتشار آنها

ورژن	زمان انتشار
Windows Server 2003	April 2003
Windows Server 2003 R2	December 2005
Windows Server 2008	February 2008
Windows Server 2008 R2	July 2009
Windows Server 2012	August 2012
Windows Server 2012 R2	October 2013
Windows Server 2016	September 2016

[1] Server Side Operating System
[2] Client Side Operating System

۱-۲ ویژگی‌ها و تغییرات جدید در ویندوز سرور ۲۰۱۶

مایکروسافت همواره به دنبال افزایش قابلیت‌ها و ایجاد بهبود در سیستم عامل‌های خود بوده است بطوری که با انتشار هر ورژن از ویندوز سرور، ویژگی‌ها و قابلیت‌های جدیدی را برای آن معرفی می‌کند. با بررسی قابلیت‌های جدید ویندوز سرور ۲۰۱۶ مشخص می‌شود که اکثر تغییرات و ویژگی‌های معرفی شده در این سیستم عامل مربوط به مباحث Cloud است که البته با گسترش استفاده از تکنولوژی‌های مجازی‌سازی[1] و سیستم‌های رایانش ابری[2] نباید انتظاری جز این از شرکت مایکروسافت (و سایر شرکت‌ها) داشته باشیم. در ادامه به بررسی اجمالی مهمترین و کاربردی‌ترین تغییرات و ویژگی‌های اعمال شده در ویندوز سرور ۲۰۱۶ می‌پردازیم. طبق اعلام رسمی شرکت مایکروسافت، این تغییرات به چهار دسته کلی تقسیم می‌شوند.

۱-۲-۱ Software-Defined Datacenter

اصطلاح SDDC[3] به این معناست که همه منابع موجود در مرکز داده یا دیتاسنتر از جمله شبکه، Storage، CPU، و ... مجازی‌سازی شده و به عنوان یک سرویس نرم افزاری (بجای سخت افزار) به مشتریان ارائه می‌شود. در این ساختار دیگر مشتریان نیاز به صرف هزینه برای خرید سخت افزار نداشته و می‌توانند همه عملیات و پردازش‌های نرم افزاری خود را از طریق وب و با استفاده از منابع اجاره شده انجام دهند. با قابلیت‌های تعبیه شده در ویندوز سرور ۲۰۱۶ این سیستم عامل گزینه‌ای بسیار مناسب برای ارائه خدمات Cloud می‌باشد.

رایانش[4]

در بخش رایانش، مایکروسافت برروی نرم افزار Hyper-V و ویژگی‌های جدید آن در ویندوز سرور ۲۰۱۶ تمرکز کرده است. به کمک نرم افزار Hyper-V می‌توان زیرساخت‌های مجازی مورد نظر را در سازمان پیاده‌سازی کرده و با ایجاد ماشین‌های مجازی[5] (VM) عملکردهای شبکه را (با مدیریت مجزا) برروی آنها میزبانی کرد.

> VMها عملکردی مشابه با سرورهای فیزیکی دارند، به عبارت دیگر، به‌جای خرید تعدادی سرور فیزیکی (جهت پیاده‌سازی سرویس‌های مختلف) می‌توان یک یا تعداد کمی سرور با سخت افزار مناسب فراهم کرده و پس از ایجاد VMها (ماشین‌های مجازی) برروی آن، سرویس‌های مورد نظر را برروی این VMها پیاده‌سازی کرد.

تغییرات ایجاد شده در ورژن ۲۰۱۶ از Hyper-V شامل موارد بسیاری بوده که آنها را به سه گروه کلی زیر تقسیم کرده‌ایم:

---

[1] Virtualization
[2] Cloud Computing
[3] Software-defined Datacenter
[4] Compute
[5] Virtual Machines

- ✓ **تغییرات نرم افزار Hyper-V:** این تغییرات مواردی همچون پشتیبانی از سخت افزارهای بیشتر و قوی‌تر، پشتیبانی از مجازی سازی تو در تو[1] (ایجاد ماشین مجازی داخل ماشین‌های مجازی دیگر)، پشتیبانی از قابلیت Secure Boot برای VMها (نوع Generation 2) با سیستم عامل لینوکس، بروز رسانی بخش Integration Services برای VMهای نوع ویندوز، ایجاد بهبود در کنسول Hyper-V Manager، محافظت از منابع اختصاص داده شده به هر VM (برای جلوگیری از استفاده توسط سایر VMها)، پشتیبانی از قابلیت Standby (در بحث مدیریت Power) در سیستم‌هایی که نرم افزار Hyper-V برروی آنها پیاده‌سازی شده است، دسترسی مستقیم VMها به سخت افزارهای نوع PCIe[2]، اجرای دستورات پاورشل[3] برروی VM به کمک سیستم میزبان VMها، و امکان فعال‌سازی قابلیت RDMA[4] برروی کارت‌های شبکه را شامل می‌شوند.
- ✓ **پشتیبانی از VM groups:** VM groups قابلیتی است که با استفاده از آن می‌توان ماشین‌های مجازی را در یک یا چندین گروه منطقی قرار داده و تغییرات (یا اقدامات مدیریتی) مورد نظر را به‌طور همزمان برروی ماشین‌های هر گروه اعمال کرد. این قابلیت در ورژن ۲۰۱۶ از ویندوز سرور پشتیبانی می‌شود.
- ✓ **تغییر در VM configuration version:** در ورژن‌های قبلی ویندوز سرور زمانی که VMها در ورژن جدیدتری از نرم افزار Hyper-V، Import می‌شدند، ورژن مربوط به پیکربندی VM به‌طور خودکار به ورژن جدید ارتقاء پیدا می‌کرد. مشکلی که در ارتقاء خودکار این ورژن‌ها وجود داشت این بود که در صورت ناسازگاری قابلیت‌های VM با ورژن جدید Hyper-V، امکان بازگرداندن آن به ورژن قبلی (ورژن اصلی) وجود نداشت. در ویندوز سرور ۲۰۱۶ این مشکل با تغییر نحوه ارتقاء ورژن‌ها از اتوماتیک به دستی برطرف شده است. به کمک این تغییر می‌توان با توجه به ورژن‌های قابل پشتیبانی توسط نرم افزار Hyper-V برروی هاست (منظور از هاست همان سروری است که Hyper-V برروی آن نصب شده است) ورژن مورد نظر را انتخاب و پیکربندی VM را به آن ارتقاء داد.
- ✓ **افزودن و حذف کردن کارت شبکه و RAM در حالت آماده به‌کار:** این قابلیت که با عنوان Hot add and remove شناخته می‌شود در ویندوز سرور ۲۰۱۶ به Hyper-V اضافه شده و به مدیران شبکه اجازه می‌دهد بدون نیاز به خاموش و یا متوقف کردن ماشین‌های مجازی، مقدار RAM اختصاص داده شده به آنها را تغییر داده و همچنین در صورت نیاز، عملیات حذف و یا اضافه کردن کارت شبکه برروی VMها را انجام دهند.

Failover Cluster

Failover Cluster قابلیتی است که به کمک آن می‌توان تعدادی سرور Hyper-V را در داخل یک گروه قرار داده (یا به اصطلاح کلاستر کرده) تا در صورت وقوع خطا در اجرای هریک از سرورها، سرور دیگری بتواند وظایف

---

[1] Nested virtualization
[2] Peripheral Component Interconnect Express
[3] PowerShell
[4] Remote Direct Memory Access

آنرا انجام دهد. این قابلیت به منظور فراهم کردن زیرســاختی قابل اطمینان و با قابلیت دســترســی بالا[1] برای پیاده‌سازی مجازی‌سازی و ایجاد سرورهای مجازی در سازمان مورد استفاده قرار می‌گیرد.

تغییرات ایجاد شده در قابلیت Failover Cluster از ویندوز سرور ۲۰۱۶ موارد زیر را شامل می‌شود:

- ✓ ایجاد quorum (کوأرِم) نوع Cloud Witness با استفاده از ویندوز Azure (آژور)
- ✓ ایجاد بهبود در دیسک‌های VHDX اشتراکی با حذف محدودیت دسترسی به زیرساخت ذخیره‌سازی و امکان گسترش فضای دیسک بدون نیاز به خاموش کردن VM
- ✓ ایجاد بهبود در لاگ‌های[2] مربوط به کلاستر
- ✓ امکان ذخیره فضای RAM درحال استفاده توسط کلاسترها (داده های موجود در RAM) برروی هارددیسک و استفاده از آنها در موقع نیاز
- ✓ ایجاد بهبود در نحوه تشخیص و عیب یابی مشکلات مربوط به نام‌ها در شبکه از طریق ارائه جزئیات کامل در مورد خطاها، امکان ارتقاء سیستم عامل سرورهای Hyper-V موجود در کلاسترها بدون نیاز به متوقف کردن کلاستر
- ✓ امکان ایجاد کلاستر برای سرورهایی که در دامین[3] یکسان یا دامین‌های متفاوت قرار داشته و یا عضوی از شبکه Workgroup هستند
- ✓ ایجاد بهبود در تعداد کانال‌های SMB[4] و امکان استفاده از چندین کارت شبکه به ازای هر سابنت[5]/شبکه در کلاستر و افزایش توان عملیاتی آن
- ✓ ایجاد بهبود در وضعیت تعادل بار[6] و همچنین ترتیب اجرای VMها در کلاستر.

Quorum تعیین کننده تعداد دفعات وقوع شکست است که یک کلاستر تا قبل از متوقف شدن قادر به تحمل آن می‌باشد. در صورتی که این تعداد شکست از مقدار تعیین شده در پیکربندی quorum تجاوز کند، کلاستر غیرفعال و متوقف می‌شود. به عنوان مثال فرض کنید ۶ سرور در یک کلاستر قرار دارند. اگر quorum برای این کلاستر با مقدار ۳ تظیم شده باشد، در صورتی که سه عدد از این سرورها در هنگام اجرا ناموفق باشند کلاستر مذکور متوقف خواهد شد.

جهت کسب اطلاعات بیشتر در رابطه با تغییرات ایجاد شده در Failover Clustering به آدرس https://blogs.msdn.microsoft.com/clustering مراجعه نمایید.

1 Highly Available
2 Logs
3 Domain
4 Server Message Block
5 Subnet
6 Load Balancing

ذخیره سازی[1]

در شبکه‌های سازمانی، معمولاً از سیستم‌های ذخیره‌سازی پیشرفته (مانند SAN storages) استفاده می‌شود. این سیستم‌ها از طریق پورت‌های فیبر نوری و iSCSI به سرورها متصل شده و از Performance (کارایی) بالایی در خصوص ذخیره‌سازی و همگام‌سازی داده‌های قابل انتقال در شبکه برخوردار می‌باشند. تغییرات و بهبودهای حاصل شده در استفاده از سیستمهای ذخیره‌سازی (در ویندوز سرور ۲۰۱۶) به چهار دسته کلی Storage Replica، Storage Spaces Direct، Deduplication، Storage Quality of Service تقسیم می‌شوند.

- ✓ **Storage Replica**: Storage Replica امکان Replication یا تکثیر Volumeها و بلوک‌های داده میان سرورهای موجود در کلاسترها و فرآیند Disaster Recovery را فراهم می‌کند. از این قابلیت در پیاده‌سازی High Availability و Failover Cluster میان دو سایت در شبکه نیز استفاده می‌شود. پیاده‌سازی Storage Replica به دو روش Synchronous (همگام) و Asynchronous (نا همگام) انجام می‌شود.
- ✓ **Storage Spaces Direct**: Storage Spaces Direct امکان استفاده از ذخیره‌سازهای Local همچون هارد دیسک‌های SATA SSD و NVMe SSD برروی سرورها را فراهم کرده، به‌گونه‌ای که با صرف هزینه‌های کمتر نسبت به سیستم‌های ذخیره سازی SAN[2] و NAS[3] می‌توان یک فضای ذخیره‌سازی با دسترسی و مقیاس پذیری بالا در اختیار داشت. این قابلیت در ویرایش Datacenter از ویندوز سرور ۲۰۱۶ قابل دسترسی است.
- ✓ **Deduplication**: Data Deduplication امکان شناسایی و حذف داده‌های تکراری ذخیره شده برروی فضای ذخیره سازی را بدون ایجاد اختلال در یکپارچگی داده‌ها فراهم می‌کند. این سرویس ابتدا به بررسی محتویات داخل Volumeها پرداخته و فایل‌های موجود برروی Volume را به تکه‌های کوچک با اندازه متغیر تقسیم می‌کند. در صورت تشخیص تکه‌های تکراری، تنها یک نسخه از آنها را برروی Volume ذخیره کرده و سایر تکه‌های مشابه را با تعدادی اشاره‌گر که به تکه‌های ذخیره‌شده ارجاع داده می‌شوند جایگزین می‌کند.
- ✓ **Storage Quality of Service**: قابلیت Storage QoS امکان نظارت و مدیریت مرکزی بر عملکرد فضای ذخیره سازی مورد استفاده توسط VMهای Hyper-V و File Server را فراهم می‌کند. در مواردی که VMها از فضای ذخیره‌سازی یکسانی استفاده می‌کنند، برای برقراری عدالت در خصوص دسترسی به این فضای ذخیره‌سازی لازم است سیاست‌هایی در رابطه با حداقل و حداکثر میزان I/O (ورودی/خروجی) انجام شده توسط هر VM انجام شود. این عملکردها توسط قابلیت Storage QoS

[1] Storage
[2] Storage Area Network
[3] Network-Attached Storage

پیاده‌سازی می‌شود.

شبکه

در دیتاسـنترهای مبتنی بر نرم افزار (SDDC)، مدیریت و نگهداری از شـبکه به کمک نرم افزارها انجام می‌شود، بنابراین هر زمان که نیاز باشد می‌توان موارد مورد نظر را ایجاد و به شبکه اضافه کرد. شبکه‌های SDN[1] در حال پیشروی به سمت سازگاری بیشتر با پلتفرم Microsoft Azure می‌باشند.

در ادامه به بررسی تغییرات ایجاد شده در بخش شبکه از ویندوز سرور ۲۰۱۶ می‌پردازیم:

- ✓ **Network virtualization**: منظور از Network Virtualization، مجازی‌سـازی سـخت افزارها و منابع سخت افزاری مورد استفاده در شبکه (مانند سوئیچ، کارت شبکه، و ...) می‌باشد. در دیتاسنترهای مبتنی بر نرم افزار، شـبکه به بخش‌هایی مجزا و ایزوله شـده تقسـیم می‌شـود و همه منابع سخت افزاری مورد نیاز شبکه در قالب سرویس‌های نرم افزاری برروی فضای میزبانی‌شده توسط میزبان دیتاسنتر نگهداری می‌شوند. در این رویکرد، به‌جای استفاده از سوئیچ، کارت شبکه، و سایر سخت افزارهای شبکه، از سوئیچ‌های مجازی، کارت شبکه مجازی و ... (که توسط Hyper-V پیاده سازی می‌شود) استفاده می‌شود.
- ✓ **Network Controller**: Network Controller به عنوان مغز راهکارهای مجازی‌سـازی شبکه درنظر گرفته می‌شـود. در شـبکه‌های بزرگ و پیچیده که بر اسـاس تکنولوژی‌های سـنتی پیاده‌سـازی شـده‌اند، خودکارسـازی اقداماتی مانند پیکربندی، نگهداری، پشـتیبان‌گیری، و عیب‌یابی سـوئیچ‌های فیزیکی شبکه با استفاده از ابزارهای مدیریت مرکزی قابل انجام است. در شبکه‌های مجازی، این اقدامات توسط Network Controller پیاده‌سـازی می‌شود. به عبارت دیگر، Network Controller با شبکه تعامل برقرار کرده و اقدامات مرتبط با نظارت و مدیریت پیکربندی‌های شـبکه را انجام می‌دهد. در این پروسـه، از نرم افزارهایی مـانـنـد System Center Operations Manager و System Center Virtual Machine Manager اسـتفاده می‌شـود. Network Controller شامل تعدادی کامپوننت است که هر کدام وظیفه مدیریت بخشی از شبکه را بر عهده دارد.
- ✓ **RAS Gateway Multitenant BGP Router**[2] : BGP[3]، یک پروتکل مسـیریابی اسـت که امکان برقرای ارتباط میان شـبکه‌های مجزا (ایزوله شـده) را فراهم می‌کند. در ویندوز سـرور ۲۰۱۶، قابلیت‌های جدیدی به RAS Gateway role اضافه شده که یکی از این موارد، پشتیبانی از BGP می‌باشد. به کمک این پروتکل امکان برقراری ارتباط و ارسـال و دریافت ترافیک میان VMهای موجود در شـبکه‌های مجزا (ایزوله شده) و همچنین برقراری ارتباط میان شبکه‌های فیزیکی و مجازی فراهم شده است.
- ✓ **Software load balancer**: Software load balancer یکی از قابلیت‌های ویندوز سرور ۲۰۱۶ است که امکان دسـترس‌پذیری و مقیاس‌پذیری بالا برای محیط‌های کاری را فراهم می‌کند. خدمات ارائه شـده

[1] Software-Defined Networking
[2] Remote Access Service
[3] Border Gateway Protocol

توسط این قابلیت، مواردی همچون: تعادل بار در لایه چهار برای انتقال ترافیک TCP/UDP، تعادل بار در ترافیک داخل شبکه و اینترنت، پشتیبانی از اختصاص آدرس پویا در VLANها و شبکه‌های مجازی فراهم شده توسط Hyper-V و تعدادی موارد دیگر را شامل می‌شود.

- ✓ **Datacenter firewall**: Datacenter Firewall یک فایروال لایه شبکه است که قابلیت‌هایی همچون: بازرسی بسته‌های Stateful، Multitenant یا محافظت از چندین VM (که به عنوان مستأجر شناخته می‌شوند)، تطبیق قانون[1] پنجگانه (بر اساس پروتکل، پورت‌های مبدأ و مقصد، آدرس IP مبدأ و مقصد). این فایروال توسط Network Controller کنترل می‌شود.
- ✓ **Web Application Proxy (WAP)**: Web Application Proxy یا به اختصار WAP، یکی از قابلیت‌های جدید ویندوز سرور است که از زمان ویندوز سرور 2012R2 به عنوان زیرمجموعه‌ای از Remote Access role ارائه گردید. به کمک این سرویس، کاربران خارج از سازمان قادر خواهند بود به Applicationها و برنامه‌های در حال اجرا برروی سرورهای داخل سازمان دسترسی پیدا کنند. در ویندوز سرور ۲۰۱۶، بهبودهایی در خصوص انتشار و دسترسی به Applicationها توسط این سرویس لحاظ شده است.

Application Platform ۲-۲-۱

در سال‌های اخیر، تغییرات قابل توجهی در خصوص پلتفرم‌های مورد استفاده برای میزبانی Applicationها در فضای شبکه و همچنین فضای Cloud ایجاد شده است. به عنوان مثال می‌توان به پلتفرم Microsoft Azure (ابر عمومی مایکروسافت) اشاره کرد. همه این پلتفرم‌ها با هدف مدرنیزه[2] کردن شبکه‌ها و انتقال از ساختار سنتی به ساختار مدرنیزه ایجاد و توسعه داده شده‌اند.

در این بخش سعی می‌کنیم به بررسی پلتفرم‌های قابل استفاده در خصوص میزبانی Applicationها در شبکه‌های مدرنیزه بپردازیم.

Microservices

مایکروسرویس‌ها نوع خاصی از رویکرد پیاده‌سازی معماری SOA[3] هستند که برای ایجاد سیستم‌های نرم افزاری مستقل و انعطاف پذیر مورد استفاده قرار می‌گیرند. در معماری هر مایکروسرویس، سرویس‌ها فرآیندهایی هستند که برای تحقق یک هدف از طریق شبکه (و پروتکل‌های ارتباطی) با یکدیگر در ارتباط هستند.

به کمک معماری فراهم شده در مایکروسرویس، Applicationها به بخش‌های کوچکتر و مستقل (اما در ارتباط با یکدیگر) تقسیم شده و هر بخش توسط یک فرایند مورد پردازش و پیاده‌سازی قرار می‌گیرد. توسعه Applicationها در معماری Microservice نسبت به SOA سریعتر انجام خواهد شد زیرا اجزا تشکیل

[1] Rule
[2] Modernizing
[3] Services-Oriented Architecture

دهنده Applicationها در Microservice بسیار کوچکتر از SOA بوده و در صورتی که نیاز به ایجاد هرگونه تغییر، به‌روز رسانی، و توسعه در این اجزاء باشد، اقدام مورد نظر به سرعت و بدون تأثیرگذاری بر سایر اجزا قابل انجام خواهد بود.

Azure

Azure (آژور)، نام پلتفرم مورد استفاده برای پیاده‌سازی ابر عمومی[1] مایکروسافت می‌باشد. به کمک این پلتفرم و قابلیت‌های تعبیه شده در آن می‌توان اکثر عملکردها و Applicationهای مورد استفاده در شبکه و سازمان (مانند Exchange Server، SQL Server، Hyper-V و ...) را برروی فضای اینترنت و Cloud در اختیار داشت.

در ویندوز سرور ۲۰۱۶ قابلیتی به نام Azure Hybrid Use Benefit (AHUB) معرفی گردید که به کمک آن می‌توان لایسنس فراهم شده برای ویندوز سرور را برروی پلتفرم Azure نیز مورد استفاده قرار داد. به عبارت دیگر می‌توان سیستم پیاده سازی شده در محیط local (که به اصطلاح on-premises نامیده می‌شود) را به محیط Cloud انتقال داد و حدود ۵۰ درصد در هزینه‌های Virtual Machineها صرفه‌جویی کرد (در Azure شما به ازای میزان استفاده خود هزینه پرداخت خواهید کرد).

Nano Server

Nano Server یک آپشن جدید برای نصب ویندوز سرور ۲۰۱۶ است که به دلیل حذف واسط‌های گرافیکی و برخی از قابلیت‌های ویندوز سرور از آن، دارای حجم بسیار پایین و سرعت پردازش بسیار بالاتری نسبت به سایر ویرایش‌های ویندوز سرور می‌باشد. این آپشن از ویندوز سرور دارای قابلیت ورود کاربران به صورت Local نبوده و مدیریت آن از طریق ابزارها و راهکارهای Remote انجام می‌شود. استفاده از Nano Server در سناریوهای زیر مناسب است:

- ✓ به عنوان سرور Hyper-V برای میزبانی از Virtual Machineها
- ✓ به عنوان File Server یا محلی برای ذخیره سازی
- ✓ به عنوان DNS Server
- ✓ به عنوان Web Server (IIS)
- ✓ به عنوان میزبان Applicationهای مبتنی بر Cloud

Nano Server تنها قادر به پشتیبانی از Applicationها و ابزارهای ۶۴ بیتی می‌باشد.

Service branching

در ورژن‌های قبلی، خدمات رسانی و پشتیبانی ویندوز سرور بر اساس مدل "۵+۵" (۵ سال پشتیبانی اصلی و پنج سال پشتیبانی به‌صورت تمدید شده) انجام می‌شد. در ویندوز سرور ۲۰۱۶ (ویرایش‌های Desktop

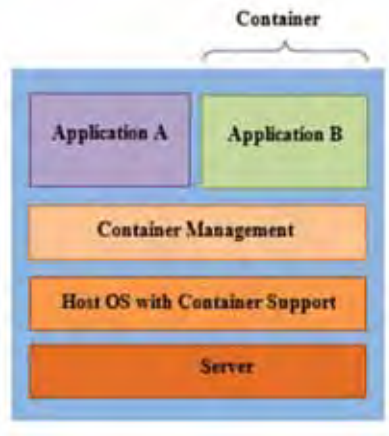
[1] Public Cloud

Experience و Server Core) نیز این روال ادامه دارد اما با نام Long-Term Servicing Branch (LTSB) شناخته می‌شود.

آن دسته از مشتریانی که از ویرایش Nano Server (و همچین ویندوز ۱۰) استفاده می‌کنند، از مدل خدمات‌رسانی فعال‌تری تحت عنوان Current Branch for Business (CBB) بهره‌مند می‌شوند. در این مدل، توسعه و به‌روز رسانی سیستم عامل (برای ارائه ویژگی‌ها و قابلیت‌های جدید) با فاصله زمانی کمتری نسب به مدل LTSB انجام می‌شود.

Containers

کانتینرها محیطی ایزوله برای اجرای Applicationها فراهم می‌کنند به گونه‌ای که عملکرد هر Application تأثیری بر سایر Applicationها و پیکربندی‌ها نخواهد داشت. به دلیل اشتراک گذاری اجزای کلیدی سیستم عامل (مانند هسته، درایوها و ...) میان کانتینرها، زمان لازم برای اجرای Applicationها در کانتینر کاهش یافته و در مقایسه با ماشین‌های مجازی (VM)، عملکرد بهینه و سریع‌تری قابل دسترسی خواهد بود.



شکل ۱-۱

۱-۲-۳ امنیت و مدیریت دسترسی[1]

در سال‌های اخیر، امنیت سایبری به عنوان یک اصل و اولویت برای سازمان‌ها در نظر گرفته می‌شود. هر روز شاهد این هستیم که سازمان‌ها و شرکت‌های بسیاری (دولتی و خصوصی) به دلیل عدم وجود سیستم‌های امنیتی قوی، مورد نفوذ هکرها قرار گرفته به گونه‌ای که این نفوذ بعضاً تا مدت‌های طولانی نیز قابل شناسایی نمی‌باشد.

در این فصل قصد داریم به ویژگی‌های امنیتی لحاظ شده در ویندوز سرور ۲۰۱۶ بپردازیم. این ویژگی‌ها به پنج

[1] Security and Access Management

دسته کلی: VMهای محافظت شده[1]، فناوری‌های مقاومت در برابر تهدیدات[2]، فناوری‌های شناسایی تهدیدات[3]، تامین امنیت دسترسی[4]، و هویت[5] تقسیم می‌شوند. در ادامه به بررسی این ویژگی‌ها می‌پردازیم.

VMهای محافظت شده

امروزه، در اکثر سازمان‌ها و شرکت‌هایی که با تکنولوژی‌های مجازی‌سازی سرو کار دارند (مانند شرکت‌های Hosting)، انواع مختلفی از مدیران، مانند: مدیران مجازی‌سازی، مدیران فضای ذخیره سازی، مدیران شبکه، مدیران Backup و ... مشغول به فعالیت بوده که هر کدام به نحوی با VMها و فضای ذخیره‌سازی مورد استفاده توسط آنها در ارتباط هستند. در این دسته از محیط‌ها، باید راهکارهایی به منظور تأمین امنیت و محافظت از VMها در برابر مواردی همچون: حملات فیشینگ[6]، حساب‌های کاربری سرقت شده از مدیران، و حملات داخلی تعبیه شود. این راهکارها توسط Shielded VMs قابل پیاده‌سازی می‌باشد.

Shielded VMs یکی از قابلیت‌های جدید ویندوز سرور ۲۰۱۶ است که امکان محافظت از داده‌ها و وضعیت VMها در مقابل اقداماتی همچون بازرسی، دزدی، و دستکاری توسط افرادی که دارای مجوز مدیریت VMها هستند را فراهم می‌کند. برای پیاده‌سازی این قابلیت، VMها باید از نوع Generation 2 (ویندوز سرور ۲۰۱۲ و بعد از آن) که از ویژگی‌های Secure boot، UEFI firmware، و virtual Trusted Platform Module (vTPM) 2.0 پشتیبانی می‌کنند بوده و همچنین سیستم عامل میزبان Hyper-V نیز باید حداقل ویندوز سرور ۲۰۱۶ باشد.

فناوری‌های مقاومت در برابر تهدیدات

ویندوز سرور ۲۰۱۶ شامل تعدادی فناوری یکپارچه در خصوص مقاومت در برابر تهدیدات داخلی و خارجی است که به کمک آنها می‌توان امنیت شبکه را به‌گونه‌ای قابل قبول تأمین کرد. این فناوری‌ها از مواردی همچون مسدود کردن دسترسی هکرهای خارج از شبکه (که قصد دارند با استفاده از ضعف‌های امنیتی به داخل شبکه نفوذ کنند) تا مقاومت در برابر کاربران و نرم افزارهای مخرب که مجوز دسترسی مدیریت شبکه را به سرقت برده‌اند شامل می‌شود.

- ✓ **Control Flow Guard**: در ویندوز سرور ۲۰۱۶ و ویندوز ۱۰، سیستم عامل توسط قابلیتی به نام Control Flow Guard محافظت می‌شود. این قابلیت یک پلتفرم امنیتی است که امکان اجرای اکسپلویت‌ها[7] و کدهای مخرب (مانند اکسپلویت‌های Buffer overflows) برروی سیستم عامل را دشوار

[1] Shielded VMs
[2] Threat-resistant technologies
[3] Threat detection technologies
[4] Securing privileged access
[5] Identity
[6] Phishing attacks
[7] Exploits

می‌کند. به عبارت دیگر زمانی که هکر قصد دارد اکسپلویت مورد نظر را برروی سیستم عامل کامپایل[1] کند، کامپایلر برخی بررسی‌های امنیتی برروی محتویات اکسپلویت (کدها) انجام داده و در صورتی که فراخوانی‌های غیر معمول به توابع خارجی را تشخیص دهد، مانع از انجام این فراخوانی‌ها شده و در نتیجه، اجرای اکسپلویت با شکست مواجه خواهد شد.

- ✓ **Device Guard**: با وجود هزاران فایل مخرب که هر روز در حال تولید هستند، استفاده از روش‌های سنتی مانند آنتی ویروس‌ها (برای حفاظت سیستم عامل در مقابل فایل‌های مخرب) به تنهایی پاسخگو نخواهد بود. در ویندوز سرور ۲۰۱۶، از قابلتی به نام Device Guard بهره‌گیری شده است که به کمک آن می‌توان از نرم افزارهای در حال اجرا در حالت‌های Kernel mode و User mode محافظت کرد.
  در حالت محافظت Kernel، Device Guard به کمک روش‌های: امضا شدن درایورها با یک امضای شناخته شده (WHQL signed) یا قرارگیری درایورها در فهرست برنامه‌های امن، از مطمئن بودن آنها اطمینان حاصل می‌کند. چنانچه هر یک از درایورها قصد بارگذاری کدهای داینامیک و یا دستکاری کدها در حافظه شوند، از اجرای آنها جلوگیری به‌عمل خواهد آمد. در حالت محافظت User نیز می‌توان سیاست‌هایی در خصوص یکپارچگی کد[2] (CI) تعریف کرده و موارد قابل اطمینان و مجاز برای اجرا برروی سرورها را تعیین کرد.
- ✓ **Credential Guard**: Credential Guard یک قابلیت مبتنی بر مجازی‌سازی است که محیطی ایزوله برای محافظت از اسرار (مانند هَش مربوط به رمزعبورهای NTLM، حساب‌های مبتنی بر دامنه و ...) فراهم می‌کند. این محیط ایزوله تنها توسط سیستم نرم افزاری مجاز قابل دسترسی می‌باشد. ایده استفاده از Credential Guard جلوگیری از سرقت حساب‌های اعتباری است که منجر به انواع حملات عبور از هش[3] می‌شود.
- ✓ **Windows Defender**: Windows Defender قابلیت جدیدی نبوده و در ورژن‌های قدیمی تر ویندوز نیز به‌کارگیری شده است. این قابلیت، به‌صورت پیش‌فرض برروی ویندوز سرور ۲۰۱۶ نصب شده و امکان شناسایی و حذف نرم افزارهای مخرب[4] (مانند ویروس‌ها، نرم افزارهای جاسوسی[5] و ...) را فراهم می‌کند.

فناوری‌های شناسایی تهدیدات

تلاش برای پیاده‌سازی اقدامات و راهکارهای امنیتی در محیط شبکه و سازمان مسئله‌ای پر اهمیت است، اما مهمتر از آن، انجام ممیزی[6] و بررسی میزان تأثیر این اقدامات بر محیط عملیاتی می‌باشد. در ویندوز سرور ۲۰۱۶، دو آپشن جدید در زیرمجموعه‌های ممیزی معرفی شده است که بینش بیشتری در خصوص رویدادها در اختیار

[1] Compile
[2] Code Integrity
[3] Pass-the-hash
[4] Malware
[5] Spyware
[6] Audit

شما قرار خواهد داد:

- ✓ **Audit Group Membership**: این آپشـن، زیرمجموعه‌ای از رویدادهای Logon/Logoff محسـوب می‌شـود. رویدادهای این زیرمجموعه زمانی ایجاد می‌شـوند که درخواسـت ورود یا Sign-in از طریق یک PC ارائه شده و وضعیت عضویت در گروه آن مورد پرس و جو قرار می‌گیرد.
- ✓ **Audit PNP Activity**: این آپشـن در زیرمجموعـه Detailed Tracking قرار داشـته و به کمک رویدادهای موجود در این زیر دسته می‌توانید وضعیت دستگاه‌های Plug and Play متصل شده به سیستم را مشـاهده کنید. در زیر دسته Audit PNP Activity، تنها ممیزی مربوط به دستگاه‌های متصل شده با موفقیت ثبت می‌شود.

تامین امنیت دسترسی

امنیت دسـترسـی مقوله‌ای نیسـت که بتوان آنرا با یک فناوری پیاده‌سـازی کرد، بلکه لازم اسـت مجموعه‌ای از فناوری‌ها و راهکارها برای تامین این امنیت به کارگیری شـود. در ویندوز سرور ۲۰۱۶، با ترکیب دو فناوری JIT[1] و JEA[2] می‌توان راهکاری برای مدیریت سـطح دسـترسـی[3] (PAM) فراهم کرد. این راهکار به همراه سـایر اقدامات قادر خواهد بود امنیت سطح دسترسی در سازمان را تأمین و مدیریت کند.

- ✓ **Just-in-Time (JIT):** به کمک این فناوری، به هر کاربر تنها در زمان درخواسـت او مجوز دسترسی داده می‌شـود و این دسترسی برای مدت زمان مشخصی قابل استفاده خواهد بود. این فناوری تضمین می‌کند که اقدامات با استفاده از مجوز دسترسی صحیح و طی زمان تعیین شده انجام خواهند شد.
- ✓ **Just Enough Administration (JEA):** با اسـتفاده از این فناوری می‌توان میزان دسـترسـی کاربران برای انجـام یـک اقدام را تعیین کرد. به عبارت دیگر، به کمک JEA دیگر نیازی به اختصـاص مجوزهای مدیریت به حسـاب یک کاربر نبوده (که ممکن اسـت حذف این مجوزها نیز فراموش شـود) و با اسـتفاده از کنترل دسترسی مبتنی بر وظیفه[4] (RBAC) می‌توان تنها به اندازه نیاز، به کاربران دسترسی داد.

شناسایی (هویت[5])

در ویندوز سـرور ۲۰۱۶، دو سـرویس Active Directory Domain Services و Active Directory Federation Services وظیفه احراز هویت و شناسایی افراد و دستگاه‌ها در ساختار اکتیو دایرکتوری را بر عهده دارند. در ادامه به معرفی بهبودهای حاصل شده در خصوص هویت یا Identity در اکتیو دایرکتوری می‌پردازیم.

- ✓ **Active Directory Domain Services**: بهبودهای حاصـل شده در این بخش، به سه دسته زیر تقسیم

[1] Just-in-Time
[2] Just Enough Administration
[3] Privileged Access Management
[4] Role-based access control
[5] Identity

می‌شوند:

- Privileged access management: یکی از راهکارهای مورد استفاده در خصوص سرقت حساب‌های اعتباری (حساب‌های کاربری) و اجرای انواع حملات عبور از هَش و فیشینگ، مدیریت سطح دسترسی یا PAM می‌باشد. ایده استفاده از PAM در اکتیو دایرکتوری به این صورت است که ابتدا یک جنگل عاری از هرگونه اقدام مخرب پیاده‌سازی شده (این جنگل با نام bastion forest شناخته می‌شود) و حساب‌های اعتباری به‌صورت ایزوله شده در آن نگهداری می‌شود (این جنگل از طریق یک رابطه اعتماد به نام PAM Trust با جنگل اصلی ارتباط برقرار می‌کند). از آنجایی که دستیابی به این حساب‌های اعتباری از طریق سیستم مدیریت هویت مایکروسافت[1] (MIM) و با اعمال مجموعه‌ای از قوانین امنیتی برروی درخواست‌های دسترسی انجام می‌شود، دسترسی به مجوزها توسط هکرها امری دشوار خواهد بود.
- Azure Active Directory Join: Azure AD Join قابلتی است که امکان ثبت دستگاه‌های سازمان برروی Azure Active Directory را فراهم می‌کند. به کمک این قابلیت، کاربران ویندوز قادر خواهند بود از هر کجا به برنامه‌ها و منابع موجود در سازمان متصل شده و از آنها استفاده کنند. در ویندوز سرور ۲۰۱۶، قابلیت Azure AD Join دستخوش بهبودهایی در خصوص شناسایی دستگاه‌ها (چه سازمانی و چه شخصی) شده است. از جمله این بهبودها می‌توان به: دسترسی کاربران به تنظیمات مدرن (رومینگ و سفارشی سازی، تنظیمات دسترسی، اعتبارها، Backup و Restore، دسترسی به Windows Store از طریق حساب کاربری سازمانی)، دسترسی به منابع سازمانی، Single sign-on، و ... اشاره کرد.
- Microsoft Passport: Microsoft Passport یک روش احراز هویت مبتنی بر کلید است که طی یک پروسه دو مرحله‌ای انجام شده و به‌جای استفاده از رمز عبور، از الگوهای رفتاری یا پین کد[2] استفاده می‌کند. اساس این روش، استفاده از کلیدهای خصوصی و عمومی می‌باشد که کلید خصوصی برروی تراشه TPM[3] از دستگاه کاربر، و کلید عمومی نیز برروی Azure Active Directory و Windows Server Active Directory ثبت می‌شود.

✓ **Active Directory Federation Services**: سرویس ADFS امکان مدیریت اقدامات مرتبط با شناسایی و احراز هویت کاربران در هنگام اتصال آنها به منابع و برنامه‌های در حال اجرا برروی سرورهای درون سازمان یا محیط Cloud را فراهم می‌کند. بهبودهای حاصل شده در خصوص سرویس ADFS از ویندوز سرور ۲۰۱۶، بیشتر در رابطه با اقدامات شناسایی و احراز هویت کاربران در محیط Azure (یا همان Cloud) می‌باشد. تعدادی از این بهبودها عبارتند از: احراز هویت چندگانه[4]، ثبت دستگاه‌ها و اعمال سیاست‌های دسترسی برای اطمینان از تطابق آنها با سیاست‌های سازمان و کاهش خطرات بالقوه در

[1] Microsoft Identify Manager
[2] PIN Code
[3] Trusted Platform Module
[4] Multifactor authentication

دسترسی به منابع، یکپارچگی ویندوز ۱۰ و Microsoft Passport، یکپارچگی LDAP[1] برای امن‌سازی دایرکتوری‌های غیر مایکروسافتی، ایجاد بهبود در ممیزی حساب‌ها، پشتیبانی بهتر SAML[2]، سفارشی کردن آیتم‌ها در هنگام ورود، ساده کردن مدیریت رمز عبورها برای کاربران Office 365، پیکربندی سیاست‌های مرتبط با کنترل دسترسی، و مهاجرت از ورژن‌های قبلی ADFS به ورژن جدید اشاره کرد.

۱-۲-۴ مدیریت سیستم ها

در این بخش به معرفی ابزارهای مرتبط با مدیریت سیستم در ویندوز سرور ۲۰۱۶ می‌پردازیم. این ابزارها عبارتند از: Windows PowerShell، System Center 2016، و Server Management Tools (SMT).

Windows PowerShell

Windows PowerShell یکی از ابزارهای مدیریتی مایکروسافت است که در قالب کنسول خط فرمان قابل دسترسی می‌باشد. به کمک این ابزار و قابلیت‌های تعبیه شده در آن، امکان پیکربندی و مدیریت سیستم‌ها و فناوری‌های مایکروسافتی به صورت Local و Remote فراهم شده است.

علاوه بر این، در ورژن ۲۰۱۶، امکان پشتیبانی از لینوکس نیز به PowerShell اضافه شده است بنابراین با همان واسط و دستورات استاندارد مورد استفاده در ویندوز می‌توان سیستم عامل لینوکس و محیط‌های لینوکسی را نیز مدیریت کرد. در سال‌های اخیر، استفاده از Windows PowerShell به سرعت در حال افزایش بوده و همانطور که شرح دادیم، این ابزار در حال تبدیل شدن به یک واسط مدیریتی قدرتمند برای مدیریت سیستم‌ها و فناوری‌های مایکروسافت و لینوکس می‌باشد.

ویژگی‌های جدید (یا بهبود یافته) در ورژن جدید PowerShell مواردی همچون: Package management (مدیریت و نصب بسته‌های نرم افزاری برروی ویندوز و لینوکس)، Windows PowerShell Classes (فراهم شدن قابلیت‌هایی جدید در خصوص برنامه نویسی شیء گرا در PowerShell)، Script debugging (امکان خطایابی اسکریپت‌ها در PowerShell)، و Desired State Configuration (فراهم کردن امکان پردازش، پذیرش، بازیابی، اعمال، نظارت، مقایسه، و گزارش‌دهی در خصوص اسناد پیکربندی).

System Center 2016

System Center 2016 یک بسته مدیریتی است که به صورت جداگانه برروی ویندوز سرور نصب می‌شود و تمرکز اصلی آن مدیریت ترکیبی منابع سازمان می‌باشد. منظور از مدیریت ترکیبی، امکان مدیریت محیط Cloud از داخل سازمان، و همچنین مدیریت داخل سازمان از طریق محیط Cloud می‌باشد. دو بسته Microsoft Operations Management Suite و Microsoft Intune به عنوان مکمل‌های System Center 2016 در محیط Cloud در نظر گرفته می‌شوند.

---

[1] Lightweight Directory Access Protocol
[2] Security Assertion Markup Language

System Center 2016 شـامل طیف وسـیعی از قابلیت‌های جدید اسـت که اکثر آنها برای پیاده‌سـازی Software-Defined Datacenter (SDDC) طراحی شـده‌انـد. این قـابلیت‌ها مواردی همچون: مدیریت دسـتگاه‌ها در محیط Cloud، Provisioning (آماده‌سـازی)، نظارت، خودکارسـازی، محافظت از داده و ... را شامل می‌شود.

Server Management Tools (SMT)

SMT مجموعه‌ای از ابزارهای گرافیکی تحت وب و ابزارهای خط فرمان است که برروی پلتفرم Azure میزبانی می‌شوند و امکان مدیریت ساده‌تر ویندوز سرور ۲۰۱۶ مخصوصاً ویرایش‌های Nano Server و Server Core را فراهم می‌کنند. با توجه به اینکه در دو ویرایش مذکور، امکان اسـتفاده از کنسـول‌های گرافیکی وجود ندارد، واسـط گرافیکی تحت وب می‌تواند اقدامات مرتبط با مدیریت سـرور را سـاده کند. ابزارهای تعبیه شده در SMT مواردی همچون: مدیریت Certificateها، مدیریت دسـتگاه‌ها، Event viewer، File Explorer، رول‌های تعریف شـده در فایروال، تنظیمات شـبکه، PowerShell، سرویس‌ها، Storage، و موارد دیگری را شامل شده که از لحاظ اقدامات مدیریتی قابل انجام و جزئیات قابل مشاهده در هر ابزار بهبودهایی حاصل شده است.

در این فصـل سـعی کردیم به‌صـورت اجمالی و گذرا، به بررسی قابلیت‌ها و ویژگی‌های جدید ویندوز سرور ۲۰۱۶ بپردازیم. هر یک از این ویژگی‌ها خود شـامل جزئیات بسـیاری اسـت که امکان پرداختن به آنها در قالب چند خط یا صفحه فراهم نمی‌باشد.

به‌طور کلی، پس از بررسی ویژگی‌ها اینگونه نتیجه‌گیری می‌شود که ویندوز سرور ۲۰۱۶ جهت سازگاری با پلتفرم Microsoft Azure توسـعه داده شـده اسـت و از این پس باید شاهد تحولات عظیمی در ساختار سیستم عامل‌های خانواده ویندوز سرور باشیم.

فصل ۲

نصب و ارتقاء به ویندوز سرور ۲۰۱۶

نصب ویندوز سرور برروی سرورهای شبکه یکی از اقداماتی است که همواره در آزمون‌های مایکروسافت مورد بررسی قرار گرفته است. شاید نخستین قدم برای فراگیری ویندوز سرور ۲۰۱۶ نصب آن برروی یک سرور فیزیکی یا مجازی باشد. همانند ورژن‌های قبلی، ویندوز سرور ۲۰۱۶ نیز به دو طریق Manual و Unattended (خودکار) قابل انجام است که در صورت داشتن دانش کافی در این زمینه، هر دو روش بسیار ساده خواهد بود.

در این فصل قصد داریم به بررسی مراحل نصب و ارتقاء به ویندوز سرور ۲۰۱۶ پرداخته و تعدادی از قابلیت‌های جدید در رابطه با آپشن‌های[1] نصب این سیستم عامل را معرفی می‌کنیم. به‌طور کلی مهمترین مباحث ارائه شده در این فصل عبارتند از:

- نیازمندی‌های نصب ویندوز سرور ۲۰۱۶
- نصب ویندوز سرور
- ارتقاء از ورژن‌های قبلی ویندوز سرور به ورژن ۲۰۱۶

۲-۱ پیش از نصب ویندوز سرور ۲۰۱۶

اگر پیش‌تر سیستم عامل‌هایی مانند ویندوز ۱۰ را نصب کرده باشید، عملیات نصب ویندوز سرور ۲۰۱۶ برای شما کار دشواری نخواهد بود. تفاوت‌هایی که در هنگام نصب ویندوز سرور ۲۰۱۶ باید به آن توجه داشته باشید، نیازمندی‌های سخت افزاری و همچنین انتخاب ویرایش مناسبی از سیستم عامل برحسب قابلیت‌های سرور و راهکارهای مجازی‌سازی[2] می‌باشد. در این قسمت به بررسی مواردی پرداخته می‌شود که قبل از اقدام به نصب ویندوز سرور ۲۰۱۶ لازم است مورد توجه قرار داده شوند.

۲-۱-۱ برنامه‌ریزی برای نصب ویندوز سرور ۲۰۱۶

در نسخه‌های پیشین ویندوز سرور، برنامه‌ریزی برای نصب ویندوز می‌توانست کمی دشوار باشد. مسائلی از جمله ویرایش سیستم عامل، استفاده از نسخه ۳۲ یا ۶۴ بیتی، و نصب به‌صورت GUI [3] یا Server Core از مواردی بودند که در تصمیم گیری شما برای انتخاب سخت افزارهای سرور نقش تعیین کننده‌ای داشتند. با انتشار ویندوز سرور 2012 R2 این آپشن‌ها به‌طور قابل ملاحظه‌ای کاهش یافته‌اند بنابراین تصمیم‌گیری برای نصب ورژن‌های

---

[1] Options
[2] Virtualization
[3] Graphical User Interface

جدید ویندوز سرور ساده‌تر شده است:

- ✓ ویندوز سـرور ۲۰۱۶ تنها به‌صـورت ۶۴ بیتی[1] عرضه می‌شود بنابراین نیازی به تصمیم‌گیری در مورد انتخاب نسخه ۳۲ بیتی[2] یا ۶۴ بیتی این سیستم عامل نمی‌باشد.
- ✓ تعداد ویرایش‌های قابل انتخاب در ویندوز سـرور ۲۰۱۶ سـه ویرایش اسـت که در مقایسه با ورژن‌های قبلی ویندوز سرور کاهش یافته است.
- ✓ آپشـن‌های Server Core و GUI همچنان در ویندوز سرور ۲۰۱۶ وجود دارند، همچنین آپشن جدیدی به نام Nano Server نیز به آنها اضـافه شـده است. در ویندوز سرور ۲۰۱۶ برخلاف ویندوز سرور 2012R2 امکان سـوئیچ کردن بین آپشـن‌های GUI و Server Core وجود نداشـته و آپشن Minimal Server Interface نیز حذف شده است.

۲-۱-۲ آشنایی با ویرایش‌های ویندوز سرور ۲۰۱۶

همانطور که مطلع هسـتید، شـرکت مایکروسافت سیستم عامل‌های ویندوز را در چندین ویرایش عرضه می‌نماید. انتخاب هریک از این ویرایش‌ها بسـتگی به قابلیت‌ها و کاربردهایی دارد که قرار اسـت برروی سـرور پیاده‌سـازی شوند. فاکتورهایی مانند قیمت، وظایف قابل اجرا، راهکارهای مجازی‌سازی، و راهکارهای Licensing از مواردی هسـتند که در این انتخاب باید مورد توجه قرار گیرند. در ویندوز سـرور ۲۰۱۶ دو ویرایش قابل انتخاب اسـت. این ویرایش‌ها عبارتند از:

- ✓ **Windows Server 2016 Datacenter**: از این ویرایش بیشـتر در محیط هایی که نیاز به پیاده‌سـازی مجازی سـازی در مقیاس گسـترده و همچنین محیط های مرتبط با Software-defined Datacenter (یا بطور کلی در محیط های Cloud) مورد استفاده قرار می‌گیرد. در این ویرایش همه قابلیت‌های ارائه شده برای ویندوز سـرور ۲۰۱۶ قابل دسترسی می‌باشد. تعداد ماشین‌های مجازی (VM) که در این ویرایش قابل پشتیبانی هستند بی‌نهایت ماشین می‌باشد.
- ✓ **Windows Server 2016 Standard**: ویرایش Standard برای اسـتفاده در محیط‌های معمولی ایجاد شده است بنابراین برخی از قابلیت‌های مرتبط با Virtualization و Cloud که در ویرایش Datacenter ارائه شـده اسـت را پشـتیبانی نمی‌کند. تعداد ماشـین‌های مجازی[3] (VMs) قابل پیاده‌سازی برروی ویرایش Standard دو ماشین (به صورت قانونی) می‌باشد.
- ✓ **Windows Server 2016 Essentials**: این ویرایش جزء ویرایش‌های پرکاربرد ویندوز سـرور نبوده و به دلیل بهره‌مندی از قابلیت‌های پایه ویندوز سـرور تنها برای اسـتفاده در سـازمان‌ها و شـرکت‌های کوچک با حداکثر ۲۵ کاربر و ۵۰ دسـتگاه مورد اسـتفاده قرار می‌گیرد. ویرایش Essentials برای آن دسته از کسب و

[1] x64
[2] x86
[3] Virtual Machines

کارهایی که از ویرایش Foundation ویندوز سـرور 2012R2 اسـتفاده می‌کردند مناسب است چراکه این ویرایش در ویندوز سرور ۲۰۱۶ پشتیبانی نمی‌شود.

۲-۱-۳ نیازمندی‌های نصب ویندوز سرور ۲۰۱۶

حداقل نیازمندی‌ها و مشـخصات سخت افزاری مورد نیاز برای نصب ویندوز سرور ۲۰۱۶ در جدول زیر آورده شده است. دقت داشته باشید که رعایت این نیازمندی‌ها برای نصب، ضروری می‌باشد.

جدول ۲-۱: نیازمندی‌های سخت افزاری نصب ویندوز سرور ۲۰۱۶

Hardware	Minimum Requirements
CPU	• 1.4 GHz 64-bit processor • Compatible with x64 instruction set • Supports NX and DEP • Supports CMPXCHG16b, LAHF/SAHF, and PrefetchW • Supports Second Level Address Translation (EPT or NPT)
RAM	• 512 MB (2 GB for Server with Desktop Experience installation option) • ECC (Error Correcting Code) type or similar technology
Hard Disk	• 32 GB (Windows Server 2016 does not allow ATA/PATA/IDE/EIDE for boot, page, or data drives)
Network adapter	• An Ethernet adapter capable of at least gigabit throughput • Compliant with the PCI Express architecture specification • Supports Pre-boot Execution Environment (PXE)
Other requirements	• DVD drive (if you intend to install the operating system from DVD media) *The following items are not strictly required, but are necessary for certain features: • UEFI 2.3.1c-based system and firmware that supports secure boot • Trusted Platform Module • Graphics device and monitor capable of Super VGA (1024 x 768) or higher-resolution • Keyboard and Microsoft® mouse (or other compatible pointing device) • Internet access

پشتیبانی از ۶۴ بیت

ویندوز سرور ۲۰۱۶ تنها به‌صورت ۶۴ بیتی موجود است، بنابراین هیچ ورژن ۳۲ بیتی یا x86 از این سیستم عامل وجود ندارد. از آنجایی که این سـیستم عامل ۶۴ بیتی می‌باشد لازم است نکاتی را در رابطه با راه‌اندازی سرورهای ۶۴ بیتی یادآور شویم: