

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ

«Дніпровська політехніка»



ЕЛЕКТРОТЕХНІЧНИЙ ФАКУЛЬТЕТ

Кафедра перекладу

ПЕРЕКЛАД У ГАЛУЗІ КОМП'ЮТЕРНОЇ ТЕХНІКИ

МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО САМОСТІЙНОЇ РОБОТИ

для студентів спеціальності 035 Філологія

Дніпро

2021

*За поданням методичної комісії спеціальності
035 Філологія (протокол № 1 від 31.08.2021р).*

Переклад у галузі комп'ютерної техніки. Методичні рекомендації до самостійної роботи для студентів спеціальності 035 Філологія / О.В. Щуров. – Дніпро, 2021. – 30 с. – Режим доступу: https://pereklad.nmu.org.ua/ua/comp_tech.pdf

Автори:

Щуров О.В. – ст. викладач

Методичні матеріали призначені для студентів спеціальності 035 Філологія які здобувають кваліфікаційний рівень бакалавра.

Матеріали стануть у пригоді для практичних робіт студентів під час підготовки до практичних занять та контрольних заходів з дисципліни «Переклад у галузі комп'ютерної техніки».

Методичні рекомендації з навчальної дисципліни «Переклад у галузі комп'ютерної техніки» для студентів, містять інструкції для виконання самостійної роботи, текстві джерала відкритого характеру з посиланнями у якості довідникового матеріалу, які повинні бути опрацьовані та використані під час виконання галузевого перекладу українською мовою. Призначено для студентів-бакалаврів освітньо-професійної програми «Германські мови та літератури (переклад включно), перша – англійська» спеціальності 035 «Філологія».

ЗМІСТ

Вступ.....	4
Інструкції до виконання самостійної роботи.....	5
Part One. Microsoft Inc. Products, Services, and Documents.....	7
Part Two. Cisco. Products, Services, and Documents.....	17

ВСТУП

Мета вивчення дисципліни «Переклад у галузі комп'ютерної техніки» – надання знань і умінь, необхідних для опанування професійних завдань (компетенцій) бакалавра, пов'язаних з усвідомленням студентом особливостей перекладу з англійської на українську мову у галузі комп'ютерних та інформаційних технологій; досягнення здобувачами вищої освіти системи спеціальних знань у галузі спеціального перекладу та теоретичних основ у визначеній галузі, які проявляються у здатності використовувати набуті знання в професійній перекладацькій діяльності. Формування загальних компетенцій бакалавра з цієї дисципліни потребує урахування міжпредметних зв'язків, без яких неможливе якісне виконання галузевого перекладу.

Завдання дисципліни:

1) ознайомити студентів на матеріалі англomовних науково-технічних текстів з типологічними властивостями галузевого тексту, зокрема загальними положеннями щодо рішення термінологічних завдань, з основними галузевими поняттями, корпоративними стандартами термінів, галузей їх вжитку на прикладах матеріалів компаній Microsoft та Cisco;

2) створити уявлення про предмет як систему взаємопов'язаних елементів з урахуванням міждисциплінарних зв'язків;

3) сформуванати навички перекладу у відповідності до стандартів та вимог компаній;

4) розвинути вміння долати термінологічні, лексико-граматичні та стилістичні, логічні та інформаційні труднощі перекладу, застосовуючи адекватні перекладацькі трансформації у межах тематики комп'ютерних технологій;

5) поліпшити грамотність майбутніх перекладачів;

6) навчити самостійно вирішувати складні інформаційно-пошукові зачдачі.

Види заочно-дистанційної роботи – письмовий переклад текстів.

Система забезпечення заочно-дистанційної роботи навчально-методичними засобами. Методичні рекомендації.

Інструкції щодо виконання завдань з самостійної роботи.

Методичні матеріали передбачають можливість проведення контролю з боку викладача.

ІНСТРУКЦІЇ ДО ВИКОНАННЯ САМОСТІЙНОЇ РОБОТИ

1. Перед виконанням перекладу фрагментів тексту зверніть обов'язкову увагу на посилання джерела тексту онлайн на сайтах компаній Microsoft та Cisco. Не виконуйте переклад фрагменту одразу, оскільки в методичних вказівках та матеріалах надано тексти різних жанрових категорій. Отже потрібно ознайомитися з ПОВНИМ текстом для визначення подальших перекладацьких труднощів, зокрема термінологічних.

2. Для елементів інтерфейсів, програмного забезпечення та усіх інших продуктів Microsoft необхідно дотримуватися термінологічних вимог і стандартів компанії. Задачу полегшено через Microsoft Language Service і він є обов'язковим для використання, оскільки один термін у різних версіях одного й того ж продукту перекладається по-різному. Посилання: <https://www.microsoft.com/en-us/language>

3. При опрацюванні термінів за тематикою Cisco необхідно виконувати пошук аналогів українською на сайті та блогах компанії cisco.com, користуючись не тільки сторінками сайту, а ще й документацією у форматі pdf та пошуком по сайту. Якщо не знайшли аналогу, утворюємо робочий термін або використовуємо стандартизований у галузі.

4. Терміни мають відбиратися за 3 принципами:

- частотність (базовий термін+усі похідні в усьому документу, а не у наведеному фрагменту для перекладу. Напр.: security – security awareness – cloud security тощо);
- контекст (значення терміну та його аналог добираються відповідно до усіх контекстів оригінального документу);
- український аналог відповідно до стандартів виробника у базовій та супутній тематиках (напр.: маршрутизатор+маркетинг).

5. Усі текстові фрагменти мають бути виконані у програмі SDL Trados або у вигляді білінгви у форматі doc:

Оригінал	Переклад

6. Якщо текст містить графіки або малюнки, мають перекладатися тільки ті надписи, які мають інформативне значення. Вони виписуються також у виді білінгви з перекладом:

RnP Connect – Підключення RnP.

Якщо напис не містить інформативного компоненту, напр. назви продуктів, компаній, форматів файлів, скорочення, які не можуть бути перекладені та є стандартизованими у компанії або галузі, то їх додавати до білінгви не потрібно.

7. Що враховується:

- відсутність логічних та змістовних помилок;

- дотримання корпоративної та галузевої термінології;
- урахування міжгалузевих зв'язків;
- читабельність тексту перекладу та урахування стилістичних особливостей кожного тексту окремо.

PART ONE

MICROSOFT INC. PRODUCTS, SERVICES, AND DOCUMENTS

Text 1

Source: <https://blogs.windows.com/windowsdeveloper/2021/06/24/what-windows-11-means-for-developers/>

With Windows 11, we are embracing all your apps and are working to make all apps feel right at home on Windows. And, with the new PWABuilder3, you can build a PWA from your web app in minutes. The evergreen WebView2 runtime is also included with Windows 11 making it easier to take advantage of its web platform as a performant and secure way to build hybrid web apps. Of course, you can continue to use powerful developer offerings like Windows Terminal and the new Microsoft Edge DevTools as they are now in-box.

The Windows App SDK, formerly known as Project Reunion, will make it easier for you to integrate Windows 11 features into your apps while still enabling you to reach more than 1B users on Windows 10. We will continue to build the Windows App SDK in cooperation with the community and starting today, you can use the Windows App SDK 0.8 Stable release (still called Project Reunion in the NuGet package and Visual Studio Marketplace). In this release you will find stability updates for WinUI3 and support for developing for Visual Studio 16.10. The Windows App SDK 1.0 will be released later this year.

You can also build apps that run natively on Windows on ARM with the new ARM64 Emulation Compatible ABI. Using the ARM64EC, you can mix native ARM and emulated x64 code in the same process or module. This interoperability means you can optimize your app to run on Windows on ARM even if your app has x64 dependencies or loads x64 plugins you don't control.

If you want to rejuvenate your app design and experiences to feel at home on Windows 11, you can use WinUI3 to take advantage of the built-in UI update such as rounded geometry, refreshed iconography, new typography, fun micro-interactions (such as Lottie animation), and refreshed color palette. New materials like Mica also add meaningful hierarchy, and more. Snap layouts will also ensure you and your users will be productive on Windows 11.

You can also easily create and manage your app's windows using Reunion Windowing. It works with your existing app code, simplifies common operations, and brings new functionality to your desktop apps like light-dismiss behavior, picture-in-picture mode, and easier titlebar customization.

Text 2

Source: <https://docs.microsoft.com/en-us/windows/mixed-reality/discover/mixed-reality>

The second one, was animating objects to sync with a capture's movement. In different parts of the app, we imported sequential OBJs of a specific capture every five frames. The OBJs were then animated in the scene to make sure they would match the corresponding frame of the capture. It's a tedious process of animating and keyframing, but the result is great. You can now see a Mixed Reality Capture interacting with non-captured objects.

When we started the UI design, we wanted to show some of the magic and possibility that holograms have to offer. Simply showing static 2D windows and text boxes doesn't feel right in the 3D world. Many of the possibilities at hand just don't show up, so right from the beginning we decided to move away from that and make full use of holographic 3D space.

At first, we started with adding some thickness to the panels, icons, and text information. Still, as a user, what I see is a text box. Text boxes with images, but we aren't there. We went further by making use of the Mixed Reality Toolkit (MRTK) shaders. The MRTK shaders became a powerful tool, and we made use of its stencil features to add negative depth to the panels. That means instead of adding elements in front of a text box, the icons now appear behind a transparent panel. What I see now as a user is something that I just can't replicate anymore in the real world, and this is where holographic magic started to happen. Also as a user I don't really like to read, I do a lot already in the physical world.

Obviously icons work a lot better than simple text does, to provide an even more powerful guidance, I then started creating a set of animated objects and avatars, each of them telling a tiny story about what is being done in the respective scenario and how it's being used.

Text 3

Source: <https://blogs.windows.com/windowsexperience/2021/07/01/whats-coming-in-windows-11-accessibility/>

Windows 11 offers familiar assistive technologies like Narrator, Magnifier, Closed Captions and Windows Speech Recognition to support users across the disability spectrum. Windows 11 also supports assistive technologies created by our partners including popular screen readers, magnification programs, CART services, speech commanding and other experiences.

Windows 11 also includes many improvements.

People who are blind, and everyone, can enjoy new sound schemes. Windows 11 includes delightful Windows start-up and other sounds, including different sounds for more accessible Light and Dark Themes. People with light sensitivity and people working for extended periods of time can enjoy beautiful color themes, including new Dark themes and reimagined High Contrast Themes. The new Contrast Themes include aesthetically pleasing, customizable color combinations that make apps and content easier to see.

Deaf and hard of hearing, language learners, and people in noisy or in quiet environments can enjoy redesigned Closed Caption themes that are easier to read and customize.

And, multiple sets of users can enjoy Windows Voice Typing, which uses state-of-the-art artificial intelligence to recognize speech, transcribe and automatically punctuate text. People with severe arthritis, repetitive stress injuries, cerebral palsy and other mobility related disabilities, learning differences including with severe spelling disabilities, language learners and people that prefer to write with their voice can all enjoy Voice Typing.

Ultimately, everyone can enjoy Windows' simplified design and user experience. It is modern, fresh, clean and beautiful.

Finally, I am happy to share that we have been working closely with assistive technology industry leaders to co-engineer what we call the "modern accessibility platform." Windows 11 delivers a platform that enables more responsive experiences and more agile development, including access to application data without requiring changes to Windows.

We embraced feedback from industry partners that we need to make assistive technology more responsive by design. We embraced the design constraints of making local assistive technology like Narrator "just work" with cloud hosted apps over a network. We invented and co-engineered new Application Programming Interfaces (APIs) to do both; to improve the communication between assistive technologies like Narrator and applications like Outlook that significantly improve Narrator responsiveness in some scenarios. The result is that Narrator feels more responsive and works over a network with cloud-hosted apps.

Text 4

Source: <https://blogs.windows.com/windowsexperience/2021/05/19/japanese-3d-artist-shares-his-perspectives-and-process-using-technology-to-turn-ideas-into-designs/>

“The memory, graphics performance and precision of the display are all specs that you wouldn’t expect from a laptop, so it’s very helpful,” he says. “They are second to none to a desktop PC. The laptop’s ProArt monitor is large and has a beautiful display. It’s like a studio PC that you can move around.”

This is especially useful when he has urgent 3D work to do on the go.

At home, he uses a 27-inch ProArt Display and because rendering time has to be fast, he must have ASUS graphics cards as well.

“The slightest color error in my work can affect the viewer’s impression,” he says. “When doing this as a job, it is important to check the colors in the correct working environment. When I used a different monitor, the colors sometimes looked different between the client’s PC and my PC. When creating CG for actual products, the colors of the products must be accurately represented. When creating a package design, if the color changes even slightly, it will affect the sales and brand image of the product.”

Toyoda says that while every artist chooses a PC that suits his or her working style, he appreciates the advantages of using a Windows PC.

“Most 3D artists use Windows PCs because 3D drawing and rendering is too demanding for other computers,” he says. “The advantage of a Windows PC is that you can freely choose the CPU, graphics board and memory capacity. I also appreciate that Windows supports a lot of software.”

He engages a variety of software for 3D production, such as Cinema4D (his main tool), Octane Render for rendering, Zbrush for sculpting and Marvelous Designer for cloth simulation.

“If I didn’t have these devices and software, I wouldn’t be able to do what I do. I sometimes draw 2D concept art as well as 3D, and it would be difficult to work with only analog materials for 2D work as well,” he says. “I will continue to actively use technology to create even better work.”

Text 5

Source: <https://blogs.windows.com/windowsdeveloper/2021/05/25/the-windows-developers-guide-to-microsoft-build-2021/>

There are several exciting Windows Subsystem for Linux (WSL) announcements at Microsoft Build this year. Firstly, WSL now includes support for applications to leverage your GPU on Windows, allowing you to run your Linux AI and Machine Learning scenarios directly inside of WSL.

With the popularization of ML-based experiences, we know how important it is for data science professionals to be productive through the best tools. The Windows Subsystem for Linux support for graphics processing unit (GPU) compute workflows allows data scientists to seamlessly access the GPU on the Windows host for speeding up the training of ML models.

Through WSL, you can use the same ML tools you are already familiar with in Linux to run your ML training jobs, while continuing to take advantage of the best productivity and collaboration tools provided by Windows. WSL supports all of the major CUDA-based tools for ML acceleration on NVIDIA GPUs, including frameworks that implement CUDA backends such as TensorFlow and PyTorch. It also supports the TensorFlow-DirectML package, which extends TensorFlow* by providing cross-vendor hardware acceleration for ML student workflows, enabling training and inferencing of ML models on a wide range of DirectX 12 compatible hardware. You can learn more about AI training in WSL here.

The second major WSL announcement is that we have added support for Linux GUI apps in WSL, which makes it possible to run your favorite Linux editors, tools, utilities and applications. This will greatly improve your ability to build, test, debug and run Linux applications.

Once you've installed GUI app support, you'll be able to open a WSL window and start a Linux GUI app right away, without the need to set up an X Server each time. You can learn more about support for Linux GUI applications in WSL here.

Yesterday, Qualcomm Technologies announced the Snapdragon Developer Kit, a cost-effective unit designed for developers to test and optimize their applications for the portfolio of Windows 10 on Arm-based PCs powered by Qualcomm Snapdragon compute platforms. Together with Qualcomm Technologies, we are releasing this resource, in a convenient desktop configuration, to lower the barriers of entry for developers to port their Windows 10 on Arm apps to support ARM64 natively. Independent software vendors need hardware to test native ARM64 apps running on Windows 10 on Arm, and the Snapdragon Developer Kit is a cost-effective new option for developers. Units will be sold at the Microsoft Store this summer. We're excited to see this announcement from Qualcomm Technologies this week and we'll have more share on this device at a later date.

Text 6

Source: <https://privacy.microsoft.com/en-US/privacystatement>

If you use a Microsoft product with an account provided by an organization you are affiliated with, such as your work or school account, that organization can:

- Control and administer your Microsoft product and product account, including controlling privacy-related settings of the product or product account.
- Access and process your data, including the interaction data, diagnostic data, and the contents of your communications and files associated with your Microsoft product and product accounts.

If you lose access to your work or school account (in event of change of employment, for example), you may lose access to products and the content associated with those products, including those you acquired on your own behalf, if you used your work or school account to sign in to such products.

Many Microsoft products are intended for use by organizations, such as schools and businesses. Please see the Enterprise and developer products section of this privacy statement. If your organization provides you with access to Microsoft products, your use of the Microsoft products is subject to your organization's policies, if any. You should direct your privacy inquiries, including any requests to exercise your data protection rights, to your organization's administrator. When you use social features in Microsoft products, other users in your network may see some of your activity. To learn more about the social features and other functionality, please review documentation or help content specific to the Microsoft product. Microsoft is not responsible for the privacy or security practices of our customers, which may differ from those set forth in this privacy statement.

When you use a Microsoft product provided by your organization, Microsoft's processing of your personal data in connection with that product is governed by a contract between Microsoft and your organization. Microsoft processes your personal data to provide the product to your organization and you, and in some cases for Microsoft's legitimate business operations related to providing the product as described in the Enterprise and developer products section. As mentioned above, if you have questions about Microsoft's processing of your personal data in connection with providing products to your organization, please contact your organization. If you have questions about Microsoft's legitimate business operations in connection with providing products to your organization as provided in the standard Microsoft Online Services Terms (OST), please contact Microsoft as described in the How to contact us section. For more information on our legitimate business operations, please see the Enterprise and developer products section.

Text 7

Source:

<file:///C:/Users/User/Downloads/Compliance%20letter%20January%202019%20with%20signature%20v2.pdf>

Hardware Recycling

Microsoft is in compliance with global electronics recycling laws, including the EU Waste Electronic and

Electrical Equipment (WEEE) Directive (2002/96/EC) and the WEEE Recast (2012/19/EU) and other electronics recycling laws in Asia, Latin America and North America. Compliance includes fulfilling recycling obligations and meeting information and labeling requirements for covered Microsoft products. To identify a location to properly dispose of Microsoft hardware devices, please consult the recycling website.

US Consumer Product Safety Improvement Act/EU Safety of Toys (Directive 2009/48/EC)

Enacted in August 2008, the US Consumer Product Safety Improvement Act of 2008 (CPSIA) limits the use of lead and certain phthalates in children's products. Although our devices are not classified as children's products, Microsoft designs its Xbox video game consoles and Xbox accessories to meet CPSIA substance restriction requirements due to their potential use by children. For the same reason, Microsoft also designs its Xbox video game consoles and Xbox accessories to meet the substance requirements of the EU Toy Safety Directive (2009/48/EC).

California Proposition 65

Proposition 65, the Safe Drinking Water and Toxic Enforcement Act of 1986, was enacted as a ballot initiative in November 1986. The Proposition was intended by its authors to protect California citizens and the State's drinking water sources from chemicals known to cause cancer, birth defects or other reproductive harm, and to inform citizens about exposures to such chemicals. None of Microsoft's products contain chemicals in amounts that would trigger a notification or warning under California Proposition 65.

Ozone Depleting Substances (ODSs)

The Montreal Protocol on Substances that Deplete the Ozone Layer ("Montreal Protocol") restricts the use of ODSs in manufacturing and Sections 4681 and 4682 of the US Internal Revenue Code (IRC) impose an excise tax on the sale or use of ODSs by the manufacturer, producer or importer of the ODS and the sale or use in the United States by the importer of any "imported taxable products." Any importation of ODSs or products containing ODSs are subject to the IRS excise tax. To ensure compliance, Microsoft has established

a strong company policy on prohibiting the use of ODSs in the manufacture of Microsoft devices.

Text 8

Source: <https://news.microsoft.com/2021/01/19/cruise-and-gm-team-up-with-microsoft-to-commercialize-self-driving-vehicles/>

To unlock the potential of cloud computing for self-driving vehicles, Cruise will leverage Azure, Microsoft's cloud and edge computing platform, to commercialize its unique autonomous vehicle solutions at scale. Microsoft, as Cruise's preferred cloud provider, will also tap into Cruise's deep industry expertise to enhance its customer-driven product innovation and serve transportation companies across the globe through continued investment in Azure.

Microsoft will join General Motors, Honda and institutional investors in a combined new equity investment of more than \$2 billion in Cruise, bringing the post-money valuation of Cruise to \$30 billion.

"Advances in digital technology are redefining every aspect of our work and life, including how we move people and goods," said Satya Nadella, CEO, Microsoft. "As Cruise and GM's preferred cloud, we will apply the power of Azure to help them scale and make autonomous transportation mainstream."

"Microsoft is a great addition to the team as we drive toward a future world of zero crashes, zero emissions and zero congestion," said GM Chairman and CEO Mary Barra. "Microsoft will help us accelerate the commercialization of Cruise's all-electric, self-driving vehicles and help GM realize even more benefits from cloud computing as we launch 30 new electric vehicles globally by 2025 and create new businesses and services to drive growth."

In addition, GM will work with Microsoft as its preferred public cloud provider to accelerate its digitization initiatives, including collaboration, storage, artificial intelligence and machine learning capabilities. GM will explore opportunities with Microsoft to streamline operations across digital supply chains, foster productivity and bring new mobility services to customers faster.

Text 9

Source: <https://www.microsoft.com/en-us/surface/devices/surface-duo?activetab=techSpecs>

Battery Capacity	3577mAh (typical) dual battery ³
Battery charging	Battery charging using 18W in box power supply
Camera and video recording	Adaptive camera 11MP, f/2.0, 1.0 μ m, PDAF and 84.0° diagonal FOV optimized with AI for front and rear
Photos	Auto mode with low-light & HDR multi-frame photo capture and dynamic range scene detection
	Super resolution zoom, and super zoom up to 7x
	Portrait mode with adjustable depth control
	Panorama mode
	Burst mode
	Video recording:
	4K video recording at 30 fps and 60 fps
	1080p video recording at 30 fps and 60 fps
	HEVC and H.264 video recording formats
	Gyro-based digital video stabilization

Standby Time: Testing conducted by Microsoft in July 2020 in an AT&T Validated Lab using preproduction Surface Duo units and software. Testing conducted in accordance with AT&T requirements and test specifications. All settings were default, and network settings were: connected to LTE, and Wi-Fi was enabled but not connected. Battery life varies significantly with network and feature configuration, signal strength, settings, usage and other factors. Battery has limited recharge cycles and cannot be replaced.

Talk Time: Testing conducted by Microsoft in July 2020 in an AT&T Validated Lab using preproduction Surface Duo units and software. Testing conducted in accordance with AT&T requirements and test specifications. All settings were default, and network settings were: connected to LTE, and Wi-Fi was enabled but not connected. Battery life varies significantly with network and feature configuration, signal strength, settings, usage and other factors. Battery has limited recharge cycles and cannot be replaced.

[3] Specified minimum dual battery capacity is 3462mAh.

[4] Network availability and coverage vary by carrier. See your carrier for details.

Text 10

Source: <https://www.microsoft.com/security/blog/2021/03/02/microsoft-unifies-siem-and-xdr-to-help-stop-advanced-attacks/>

For all of us in security, the last twelve months have been an incredible series of challenges—from balancing remote work with family priorities, to helping build resilient businesses, and protecting against the latest attacks. 2020 showed us that while we have made great progress, there is still a lot we can do as individuals, organizations, and as a community to keep secure. Here at Microsoft, we're committed to applying these learnings to help create a stronger, more unified approach to security for all—no matter what platform you're on, device you're trying to protect, or cloud your data is in.

To help protect against advanced attacks, last September at Microsoft Ignite we shared our vision to create the most complete approach to securing your digital landscape, all under a single umbrella. We combined the breadth of Azure Sentinel, our cloud-native SIEM (security information and event management) with the depth of Microsoft 365 Defender and Azure Defender, our XDR (extended detection and response) tools, to help fight against attacks that take advantage of today's diverse, distributed, and complex environments.

Today we are taking the next step in unifying these experiences and delivering enhanced tools and intelligence to stop modern threats.

As well as unifying the capabilities of Microsoft Defender for Endpoint and Defender for Office 365 into Microsoft 365 Defender, we have also created new enhanced experiences including:

- Threat Analytics, now in preview, provides detailed threat intelligence reports from expert Microsoft security researchers that help you understand, prevent, and mitigate active threats.
- Learning Hub where you can use instructional resources with best practices and how-tos.
- Attack Simulation Training in Microsoft Defender for Office 365 which helps you detect, prioritize, and remediate phishing risks. It uses neutralized versions of real attacks to simulate the continually changing attacker landscape, enabling highly accurate and up-to-date detection of risky behavior, with rich reporting and analytics to help customers measure their progress.

With Azure Sentinel, we're focused on giving you a richer organization-wide view with expanded data collection and helping you to respond faster with new incident response and automation capabilities. Today we are announcing more than 30 new connectors to simplify data collection across your entire environment, including multi-cloud environments. These new connectors include Salesforce service cloud, VMWare, Cisco Umbrella, and Microsoft Dynamics.

PART TWO

CISCO. PRODUCTS, SERVICES, AND DOCUMENTS

Text 1

Source: https://www.cisco.com/c/dam/m/en_us/solutions/smart-building/nb-06-smart-building-technologies-guide/Smart-Building-Guide.pdf

Creating a trusted workplace means making users feel safe. Fortunately, IoT devices are good at this. They excel in providing a sense of security to smart building users while also being functional. Cameras, sensors, badge readers, and other devices can all coordinate to provide more accurate and timely data for better decision making. They can also implement automated policies and controls to restrict access or provide a predetermined response based on user behaviors. By leveraging technology as a force multiplier, building operators can do an end run around budget and staffing constraints. Smart buildings are best known for their promotion of security- and safety-related environmental controls and building automation systems. Depending on a facility's use, these could be deemed mission critical (e.g., healthcare, research, utilities). These systems can be enhanced to protect the health of users via apps for social distancing and contact tracing, and even for automated disinfection. More important, these solutions can be applied to existing buildings to mitigate various risks, including to health, while ensuring business continuity. A smart building's network must also provide end-to-end threat-centric security, including for all connected end devices. Establishing a proactive defense that searches for threats or issues before they take hold prevents downtime and loss of services. Plus, it keeps facilities operating at peak efficiency. But more important, it keeps facility and user data secure.

With 90W Universal Power over Ethernet Plus (UPOE+), available through solutions like Cisco® Catalyst® 9000 switches, smart buildings deliver DC power to devices over copper Ethernet cabling, eliminating the need for separate power supplies and outlets.

UPOE+ lets building operators gain unprecedented flexibility to design workspaces around users, not outlets. This can return a 30-percent reduction in electrical materials costs.

By using a DC microgrid with UPOE+, you can eliminate conversion losses from AC to DC, resulting in savings at every load. Smart buildings can often provide a 45-percent improvement in energy efficiency through the use of DC power.

Text 2

Source: <https://www.cisco.com/c/en/us/products/collateral/wireless/dna-spaces/datasheet-c78-741786.html#Productcapabilities>

Cisco DNA Spaces supports all Cisco wireless topologies with compatibility and interoperability across Cisco Aironet, Cisco Catalyst, and Cisco Meraki products and solutions (see Figure 2).

How to connect:

1. Use Cisco DNA Spaces Connector to connect to Cisco Aironet WLC 8.0 and Cisco Catalyst 9800 Series WLC 16.12.1 and above – This is the recommended approach to connect a Wireless LAN Controller based network.
2. Directly connect Meraki networks to Cisco DNA Spaces cloud via cloud-to-cloud integration.
3. Tether CMX on-prem 10.6 or later, but this does not support all the use cases, so Cisco DNA Spaces connector is recommended.

When is CMX on premises required?

An on premises CMX server is required for customers that have an air-gapped installation or using automatic integration with Cisco Prime. For all other use cases including automatic integration with Cisco DNA Center, CMX is not required.

4. For some limited deployments you can directly connect Cisco Catalyst 9800 Series WLC 16.12.1 and above or AireOS WLC 8.5 or above to Cisco DNA Spaces cloud

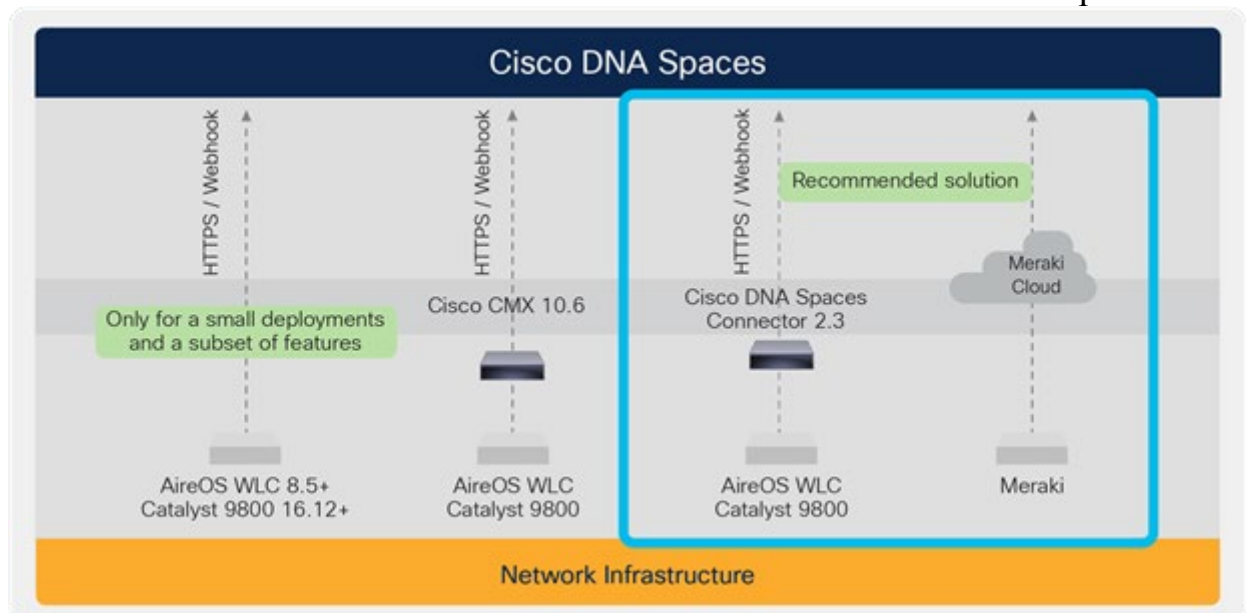


Figure 2.

Compatible across All Network Infrastructure

Text 3

Source: <https://www.cisco.com/c/en/us/products/collateral/software/smart-accounts/guide-c07-744931.html>

You have four deployment choices with Smart Licensing. Use one across your organization or mix and match as you like.

- **Direct licensing management and reporting**

This cloud-based deployment method is our simplest. If your Cisco products are connected to tools.cisco.com via the internet or HTTP proxy server, those devices will automatically report usage information. Direct deployment works out of the box with no additional configuration required.

- **On-premises license management and reporting**

This deployment method is best when security policies require devices to be isolated from the internet. Device communication is contained within the local network. The on-premises server uses a synchronization process to exchange license information with the Cisco Smart Software Manager. Transfers can be automatic and network based or offline and manual. This method simplifies larger Cisco deployments (of roughly 30 or more licenses). Read the data sheet to learn more.

- **Disconnected (license reservation) license usage**

This is our highest level of security for organizations that need a full air-gapped environment (and on-premises licensing isn't an option). Access through license reservation is fully offline and requires no ongoing communication or additional infrastructure. All licenses are manually checked in and out by copying and pasting information between products and Cisco.com. Disconnected licensing works well for remote deployments.

- **Plug and Play**

Improve operational efficiency with a simple, secure, and integrated method for device onboarding.

With Cisco Network Plug and Play, you can secure and scale with a cloud-based service that provides a mechanism for discovering a network device with on-premises Cisco DNA Center or Cisco DNA Center Cloud. It's the go-to solution for simple day-zero provisioning across all Cisco enterprise platforms (routers, switches, and wireless access points). Plug and Play requires a Smart Account during device procurement.

- **Get started with Network Plug and Play**

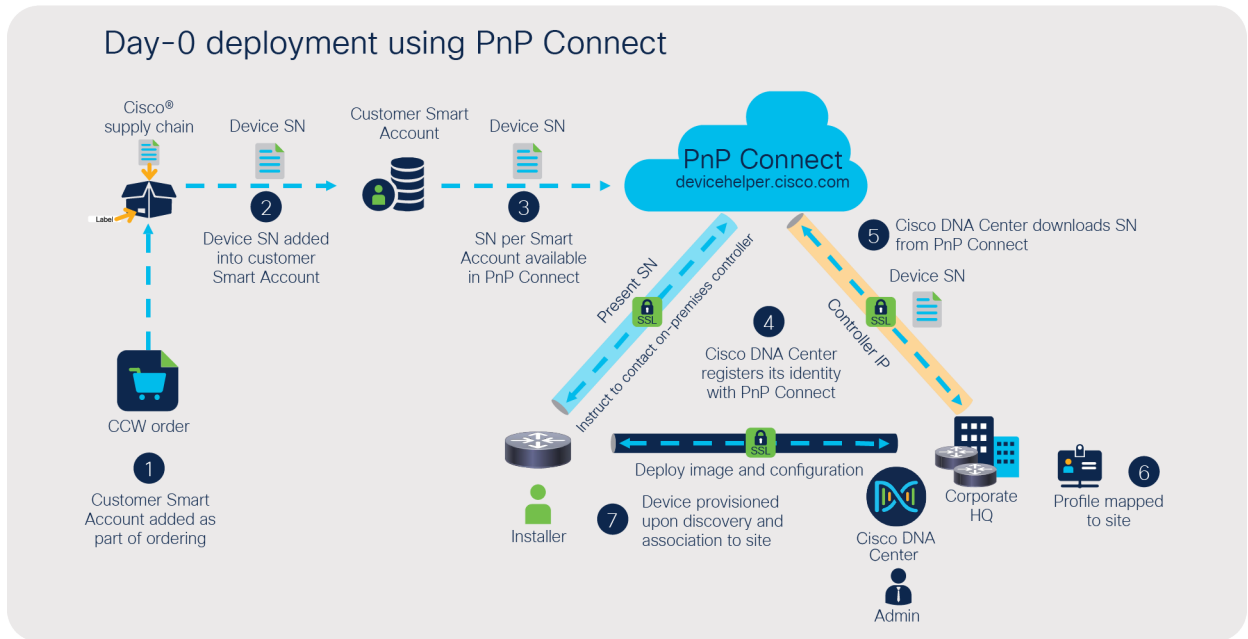


Figure 1.

Components overview

Text 4

Source: <https://blogs.cisco.com/security/top-tips-for-ransomware-defense>

If you're not sure where to begin with ransomware defense, start with basic cyber hygiene. (While some of this may sound simplistic, it's often overlooked due to resource constraints, a focus on higher-level projects, and so on. Attackers are aware of this and often exploit these common vulnerabilities and weaknesses).

Keep systems patched and updated. Automated patching, when feasible, can help ensure that nothing slips through the cracks, and can also lessen the burden on your IT and security teams. Out of the 25 best practices we analyzed in our 2021 Security Outcomes Study, it was found that proactively refreshing technology had the strongest effect on improving overall defenses.

Always back up data so that it can be recovered in an emergency. Store backups offline so they cannot be found by cyber intruders. Develop a data recovery plan that can help you achieve restoration at scale while ensuring business continuity.

Maintain an accurate and up-to-date inventory of your assets. Older, forgotten machines often provide a way in for attackers.

Conduct ongoing risk assessments to uncover any vulnerabilities in your infrastructure. Encrypt confidential data, and segment your network so that cybercriminals cannot easily get to critical systems.

Make sure your employees are familiar with cybersecurity and ransomware. Train them on the importance of strong passwords, how to spot a phishing email, what to do if they receive a suspicious communication, and so on.

Stay informed about the latest risks and defensive tactics, and have a solid incident response plan in place to handle unexpected threats. Organizations like Cisco Talos offer incident response services to help you prepare for, respond to, and recover from breaches. Pay attention to ransomware guidance from government entities such as CISA and NIST.

Technologies that can help

And of course, be sure to implement a comprehensive range of security solutions to cover the many threat vectors attackers use to get in, including:

- Next-generation firewall and IPS – Prevent attacks from invading your network with modernized firewall and intrusion prevention technology.

- Email security – Block ransomware delivered via spam and phishing, and automatically identify malicious attachments and URLs.
- Cloud & web security – Protect users from ransomware and other malware while they're on the Internet or using cloud applications.
- Endpoint protection – Detect and remediate threats that infect the various endpoints across your environment.
- Secure access – Ensure that only authorized users and devices are accessing your resources through multi-factor authentication (MFA) and other safeguards.
- Network visibility & analytics – Get a handle on what's going on in your network so that anomalous behaviors can be quickly mitigated. Employ a solution that can analyze both encrypted and unencrypted traffic.

Using these and other technologies, organizations should take a zero trust approach to security. This means that no access attempt by any person, device, or application should be implicitly trusted. Zero trust security will make it harder for cybercriminals to successfully launch ransomware across your network.

Text 5

Source: <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html>

Control Plane – LISP

In many networks, the IP address associated with an endpoint defines both its identity and its location in the network. In these networks, the IP address is used for both network layer identification (who the device is on the network) and as a network layer locator (where the device is at in the network or to which device it is connected). This is commonly referred to as *addressing following topology*. While an endpoint's location in the network will change, who this device is and what it can access should not have to change. The Locator/ID Separation Protocol (LISP) allows the separation of identity and location through a mapping relationship of these two *namespaces*: an endpoint's identity (EID) in relationship to its routing locator (RLOC).

The LISP control plane messaging protocol is an architecture to communicate and exchange the relationship between these two *namespaces*. This relationship is called an *EID-to-RLOC mapping*. This EID and RLOC combination provide all the necessary information for traffic forwarding, even if an endpoint uses an unchanged IP address when appearing in a different network location (associated or mapped behind different RLOCs).

Simultaneously, the decoupling of the endpoint identity from its location allows addresses in the same IP subnetwork to be available behind multiple Layer 3 gateways in disparate network locations (such as multiple wiring closets), versus the one-to-one coupling of IP subnetwork with network gateway in traditional networks. This provides the benefits of a Layer 3 Routed Access network, described in a later section, without the requirement of a subnetwork to only exist in a single wiring closet.

Instead of a typical traditional routing-based decision, the fabric devices query the control plane node to determine the routing locator associated with the destination address (EID-to-RLOC mapping) and use that RLOC information as the traffic destination. In case of a failure to resolve the destination routing locator, the traffic is sent to the default fabric border node. The response received from the control plane node is stored in the LISP map-cache, which is merged to the Cisco Express Forwarding (CEF) table and installed in hardware.

Text 6

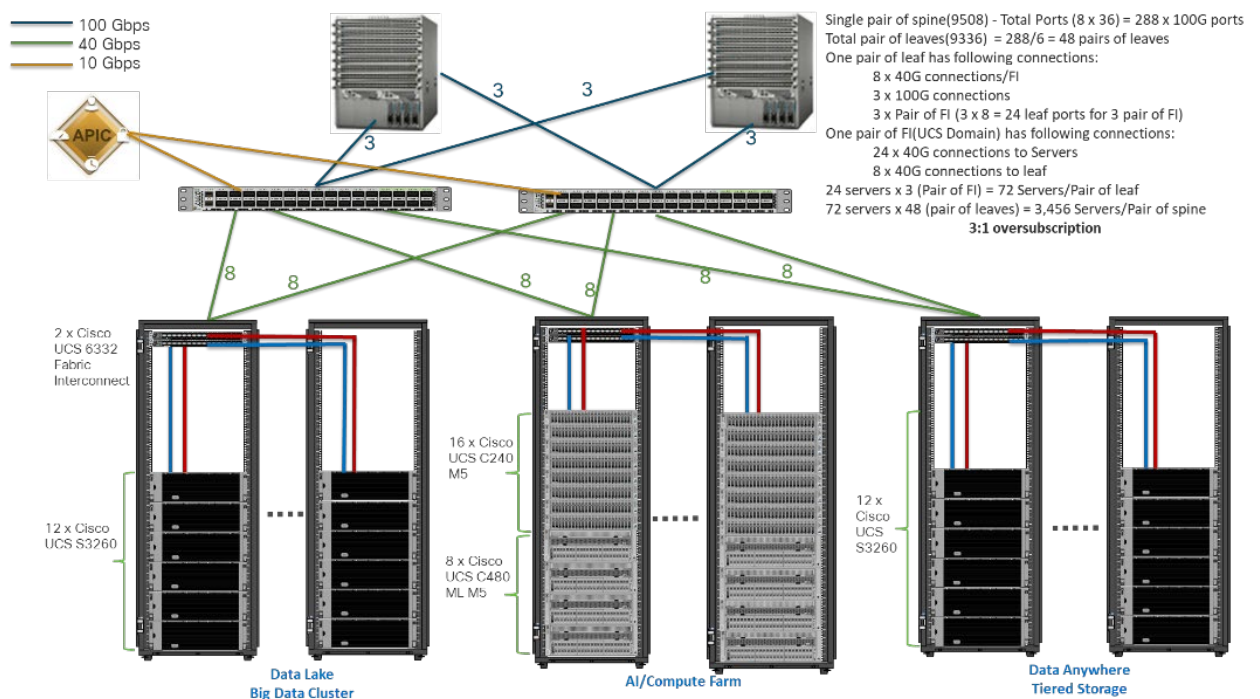
Source:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/cisco_ucs_s3_260_cdip_cloudera.html#_Toc48030064

The architecture discussed here and shown in Figure 6 supports 3:1 network oversubscription from every node to every other node across a multidomain cluster (nodes in a single domain within a pair of Cisco fabric interconnects are locally switched and not oversubscribed).

From the viewpoint of the data lake, 24 Cisco UCS C240 M5 Rack Servers are connected to a pair of Cisco UCS 6332 Fabric Interconnects (with 24 x 40-Gbps throughput). From each fabric interconnect, 8 x 40-Gbps links connect to a pair of Cisco Nexus 9336 Switches. Three pairs of fabric interconnects can connect to a single pair of Cisco Nexus 9336 Switches (8 x 40-Gbps links per Fabric Interconnect to a pair of Nexus switch). Each of these Cisco Nexus 9336 Switches connects to a pair of Cisco Nexus 9508 Cisco ACI switches with 6 x 100-Gbps uplinks (connecting to a Cisco N9K-X9736C-FX line card). The Cisco Nexus 9508 Switch with the Cisco N9K-X9736C-FX line card can support up to 36 x 100-Gbps ports, each and 8 such line cards.

Figure 6 Scaled Architecture with 3:1 Oversubscription with Cisco Fabric Interconnects and Cisco ACI



Scaled Architecture with 2:1 Oversubscription with Cisco ACI

In the scenario discussed here and shown in [Figure 7](#), the Cisco Nexus 9508 Switch with the Cisco N9K-X9736C-FX line card can support up to 36 x 100-Gbps ports, each and 8 such line cards.

Here, for the 2:1 oversubscription, 30 Cisco UCS C240 M5 Rack Servers are connected to a pair of Cisco Nexus 9336 Switches, and each Cisco Nexus 9336 connects to a pair of Cisco Nexus 9508 Switches with three uplinks each. A pair of Cisco Nexus 9336 Switches can support 30 servers and connect to a spine with 6 x 100-Gbps links on each spine. This single pod (pair of Cisco Nexus 9336 Switches connecting to 30 Cisco UCS C240 M5 servers and 6 uplinks to each spine) can be repeated 48 times (288/6) for a given Cisco Nexus 9508 Switch and can support up to 1440 servers.

To reduce the oversubscription ratio (to get 1:1 network subscription from any node to any node), you can use just 15 servers under a pair of Cisco Nexus 9336 Switches and then move to Cisco Nexus 9516 Switches (the number of leaf nodes would double).

Text 7

Source:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/cisco_ucs_s3_260_cdip_cloudera.html#_Toc48030064

To configure the Cisco UCS Fabric Interconnects, follow these steps:

1. Verify the following physical connections on the fabric interconnect:

- The management Ethernet port (mgmt0) is connected to an external hub, switch, or router.
- The L1 ports on both fabric interconnects are directly connected to each other.
- The L2 ports on both fabric interconnects are directly connected to each other

Configure Fabric Interconnect A

To configure Fabric Interconnect A, follow these steps:

1. Connect to the console port on the first Cisco UCS 6332 Fabric Interconnect.

At the prompt to enter the configuration method, enter **console** to continue.

If asked to either perform a new setup or restore from backup, enter **setup** to continue.

Enter **y** to continue to set up a new Fabric Interconnect.

Enter **y** to enforce strong passwords.

2. Enter the password for the admin user.

3. Enter the same password again to confirm the password for the admin user.

When asked if this fabric interconnect is part of a cluster, answer **y** to continue.

Enter **A** for the switch fabric.

4. Enter the cluster name for the system name.

5. Enter the Mgmt0 IPv4 address.

6. Enter the Mgmt0 IPv4 netmask.

7. Enter the IPv4 address of the default gateway.

8. Enter the cluster IPv4 address.

To configure DNS, answer **y**.

9. Enter the DNS IPv4 address.

Answer **y** to set up the default domain name.

10. Enter the default domain name.

Review the settings that were printed to the console, and if they are correct, answer **yes** to save the configuration.

11. Wait for the login prompt to make sure the configuration has been saved.

Configure Fabric Interconnect B

To configure Fabric Interconnect B, follow these steps:

1. Connect to the console port on the second Cisco UCS 6332 Fabric Interconnect.

When prompted to enter the configuration method, enter **console** to continue.

The installer detects the presence of the partner Fabric Interconnect and adds this fabric interconnect to the cluster. Enter **y** to continue the installation.

2. Enter the admin password that was configured for the first Fabric Interconnect.

3. Enter the Mgmt0 IPv4 address.
4. Answer yes to save the configuration.
5. Wait for the login prompt to confirm that the configuration has been saved.

For more information about configuring Cisco UCS 6332 Series Fabric Interconnect, go to: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Getting-Started/4-1/b_UCSM_Getting_Started_Guide_4_1.html


Log into Cisco UCS Manager

To log into Cisco UCS Manager, follow these steps:

1. Open a Web browser and navigate to the Cisco UCS 6332 Fabric Interconnect cluster address.
2. Click the Launch link to download the Cisco UCS Manager software.
3. If prompted to accept security certificates, accept as necessary.
4. When prompted, enter admin for the username and enter the administrative password.
5. Click Login to log into the Cisco UCS Manager.

Upgrade Cisco UCS Manager Software to Version 4.1(1a)

This document assumes you're using Cisco UCS 4.1(1a). Refer to the Cisco UCS 4.1 Release (upgrade Cisco UCS Manager software and Cisco UCS 6332 Fabric Interconnect software to version 4.1(1a)). Also, make sure the Cisco UCS C-Series version 4.1(1a) software bundles are installed on the Fabric Interconnects.

 Upgrading Cisco UCS firmware is beyond the scope of this document. However for complete Cisco UCS Install and Upgrade Guides, go to: <https://www.cisco.com/c/en/us/support/servers-unified-computing/ucs-manager/products-installation-guides-list.html>

Text 8

Source:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/cisco_ucs_s3_260_cdip_cloudera.html#_Toc48030064

The two main resources that Spark (and YARN) are dependent on are CPU and memory. Disk and network I/O play a part in Spark performance as well, but neither Spark nor YARN currently can actively manage them. Every Spark executor in any application has the same fixed number of cores and same fixed heap size. The number of cores can be specified with the `executor-cores` flag when invoking `spark-submit`, `spark-shell`, and `pyspark` from the command line, or by setting the `spark.executor.cores` property in the `spark-defaults.conf` file or in the `SparkConf` object.

The heap size can be controlled with the `executor-memory` flag or the `spark.executor.memory` property. The `cores` property controls the number of concurrent tasks an executor can run, `executor-cores = 5` mean that each executor can run a maximum of five tasks at the same time. The memory property impacts the amount of data Spark can cache, as well as the maximum sizes of the shuffle data structures used for grouping, aggregations, and joins.

The `num-executors` command-line flag or `spark.executor.instances` configuration property control the number of executors requested. Dynamic Allocation can be enabled from CDH5.4 instead setting the `spark.dynamicAllocation.enabled` to `true`. Dynamic allocation enables a Spark application to request executors when there is a backlog of pending tasks and free up executors when idle.

Asking for five executor cores will result in a request to YARN for five virtual cores. The memory requested from YARN is a little more complex for a couple reasons:

- `executor-memory/spark.executor.memory` controls the executor heap size, but JVMs can also use some memory off heap, for example for VM overhead, interned Strings and direct byte buffers. The value of the `spark.yarn.executor.memoryOverhead` property is added to the executor memory to determine the full memory request to YARN for each executor. It defaults to `max(384, 0.10 * spark.executor.memory)`.
- YARN may round the requested memory up a little. YARN's `yarn.scheduler.minimum-allocation-mb` and `yarn.scheduler.increment-allocation-mb` properties control the minimum and increment request values respectively.
- The application master is a non-executor container with the special capability of requesting containers from YARN, takes up resources of its own that must be budgeted in. In `yarn-client` mode, it defaults to a 1024MB and one vcore. In `yarn-cluster` mode, the

application master runs the driver, so it's often useful to add its resources with the `-driver-memory` and `-driver-cores` properties.

- Running executors with too much memory often results in excessive garbage collection delays. 64GB is a rough guess at a good upper limit for a single executor.
- A good estimate is that at most five tasks per executor can achieve full write throughput, so it's good to keep the number of cores per executor around that number.
- Running tiny executors (with a single core and just enough memory needed to run a single task, for example) throws away the benefits that come from running multiple tasks in a single JVM. For example, broadcast variables need to be replicated once on each executor, so many small executors will result in many more copies of the data.

Для нотаток

Навчальне видання

Щуров Олексій Вікторович

ПЕРЕКЛАД У ГАЛУЗІ КОМП'ЮТЕРНОЇ ТЕХНІКИ

Методичні рекомендації до самостійної роботи
для бакалаврів спеціальності 035 Філологія

Електронний ресурс

За редакцією укладача