

Exam AZ-500: Microsoft Azure Security Technologies Crash Course



Tim Warner



Tim Warner



- Based in Nashville, TN, US
- MCT, MVP
- Twitter: [@TechTrainerTim](#)
- Badge: [timw.info/sec](#)



Course Materials

timw.info/az500

Session 1 of 2 Learning Goals

- Introduction
- Manage identity and access
 - Administer Azure AD security
 - Configure Azure AD PIM
- Implement platform protection
 - Configure network, container, host security
- Manage security operations
 - Configure Azure Security Center
 - Configure Azure DevOps

Session 2 of 2 Learning Goals

- Manage security operations, continued
 - Configure security policies
 - Configure security alerts
- Secure data and applications
 - Configure data classification
 - Protect data infrastructure
 - Configure application security and Key Vault

Setting Expectations

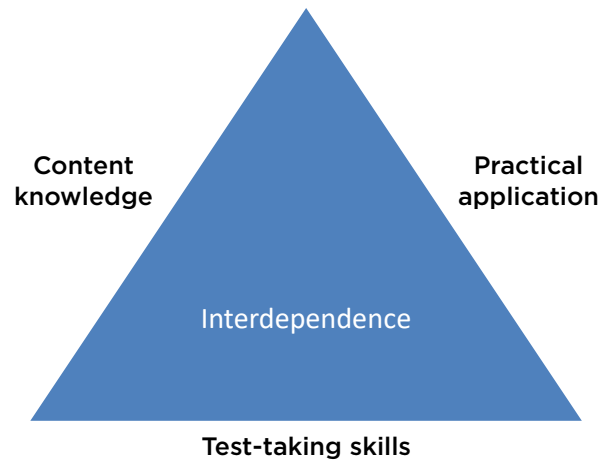
- The job role in play is the Azure Security Administrator
 - Identify which security controls are available for different Azure products and know their configuration basics
- This is a "crash course"
 - Plan to review these materials more than once
 - Five-minute break at midpoint
- Please ask/answer questions and provide feedback in the Q/A panel, not the group chat

2020 Certification Updates

- Microsoft Worldwide Learning reviews each role-based certification yearly
- Exam AZ-500 will be updated on July 29, 2020
 - Review the "Skills Measured" document:
<https://timw.info/500sm>
- Themes:
 - Eliminated redundancy with other exams
 - Reorganized outline
 - Azure Sentinel
 - Removed references to legacy technologies (HDInsight)

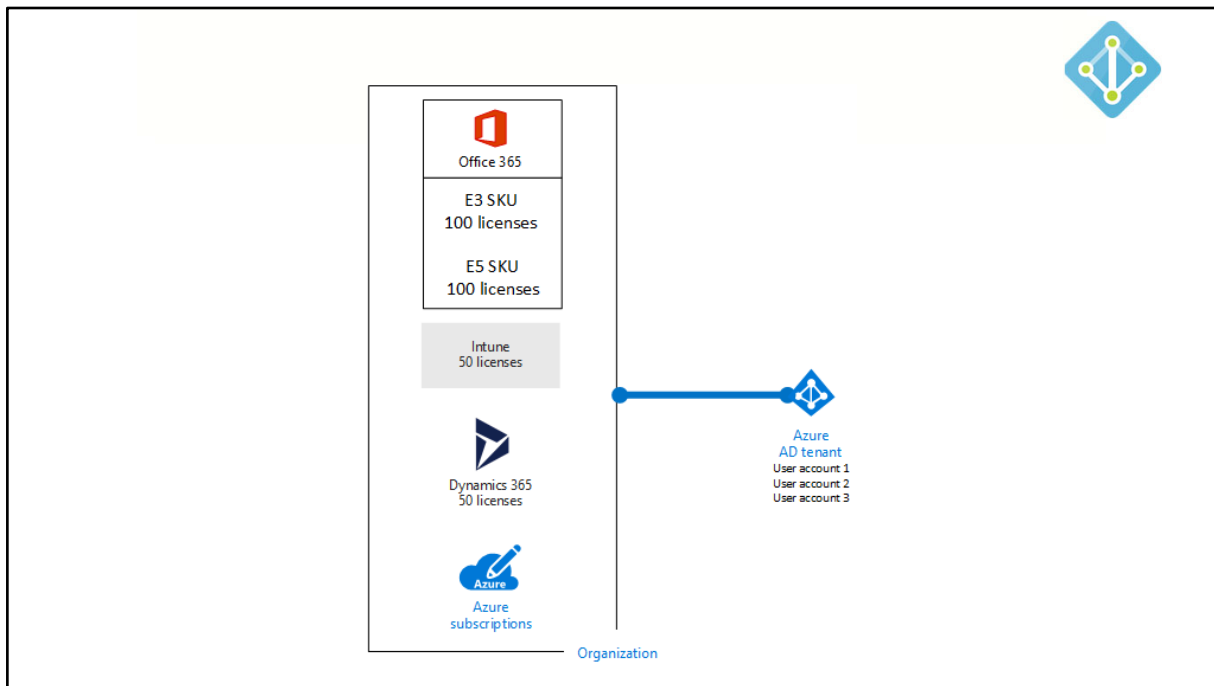


Tim's Certification Study Pyramid

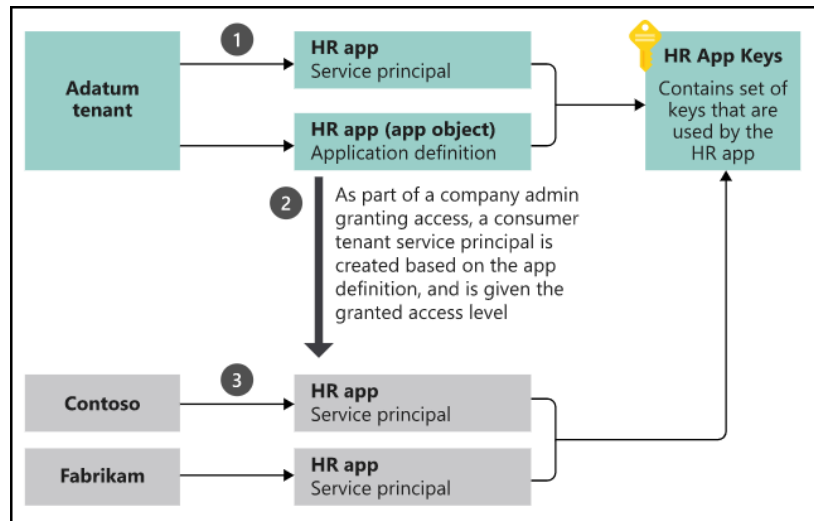


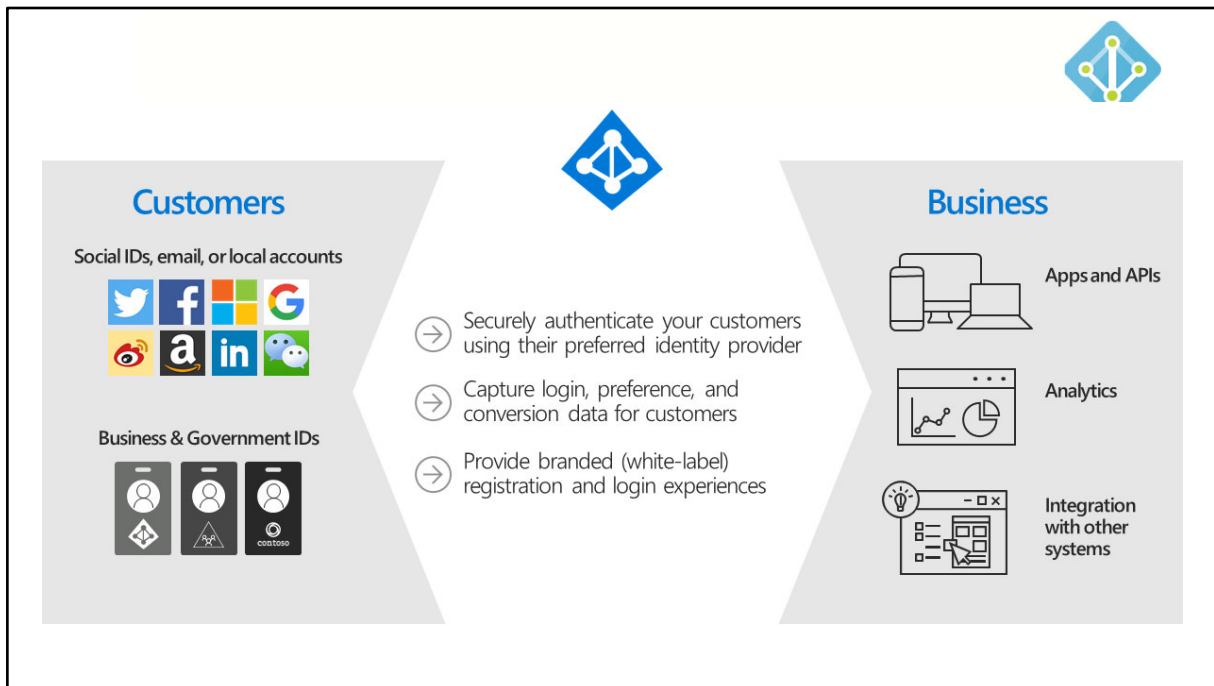


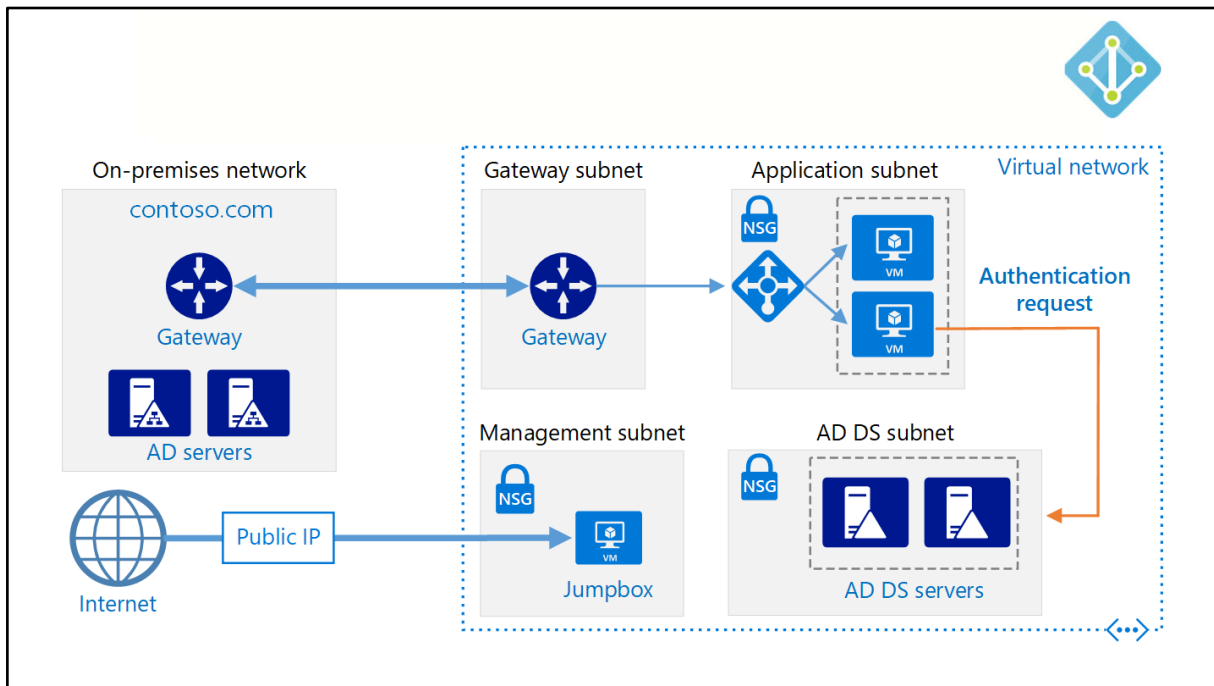
Manage Identity and Access

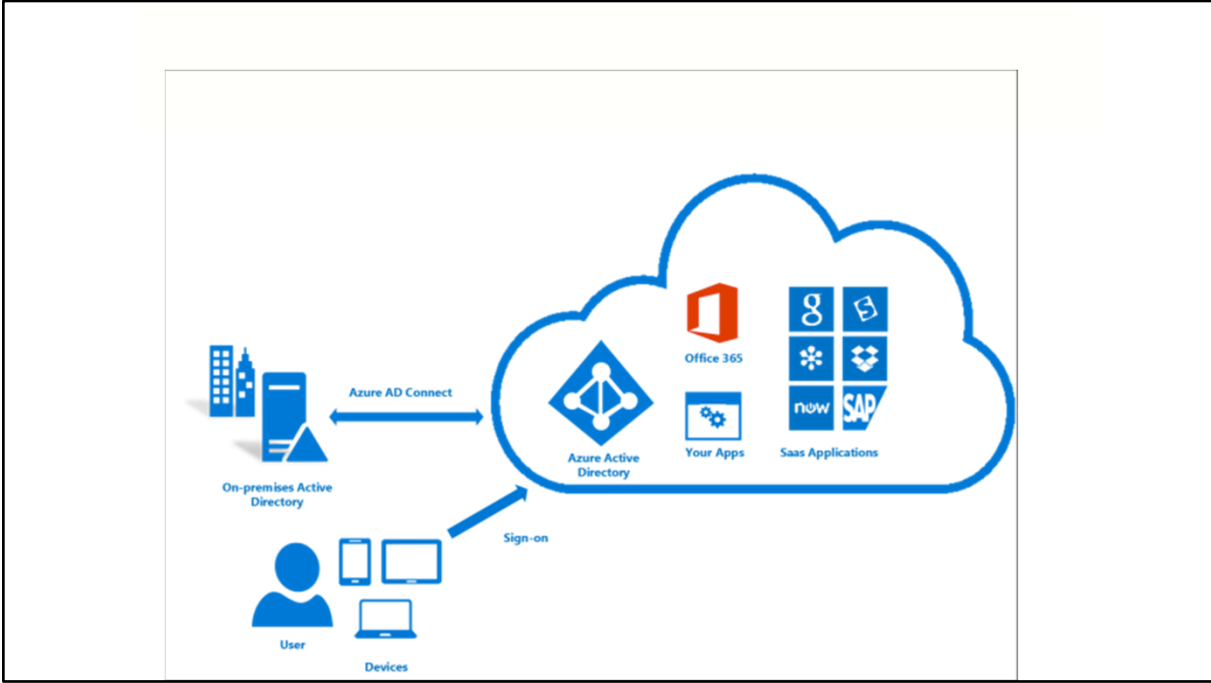


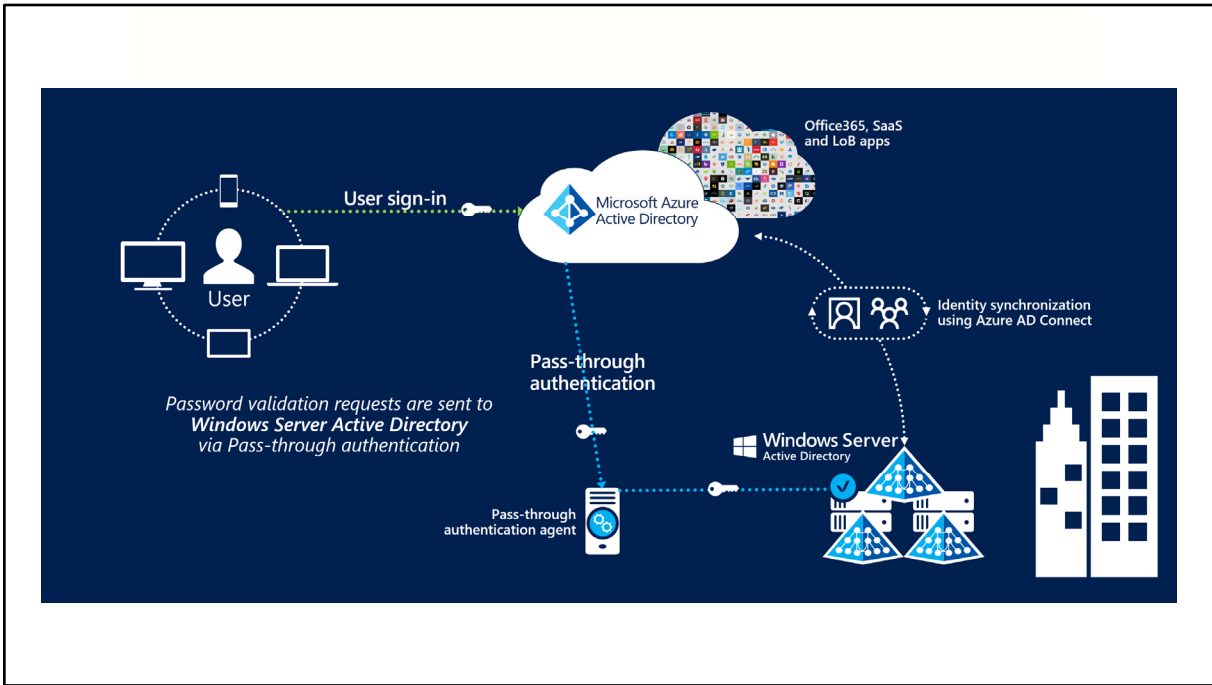
App registrations and service principals

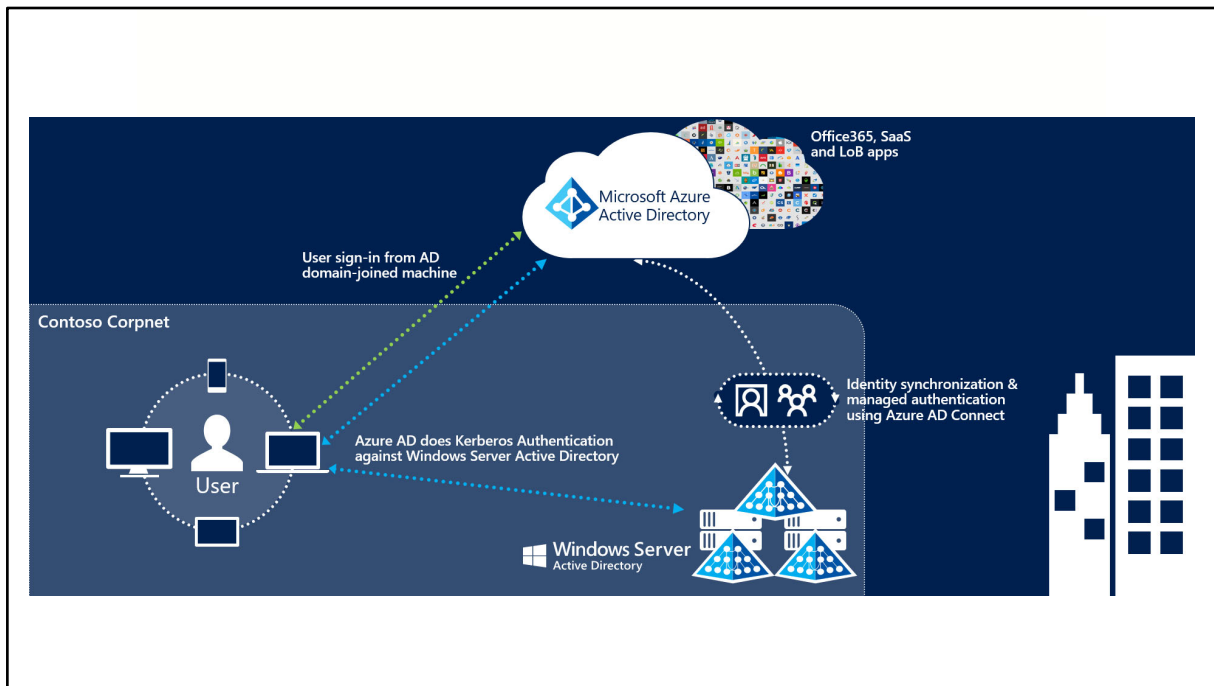




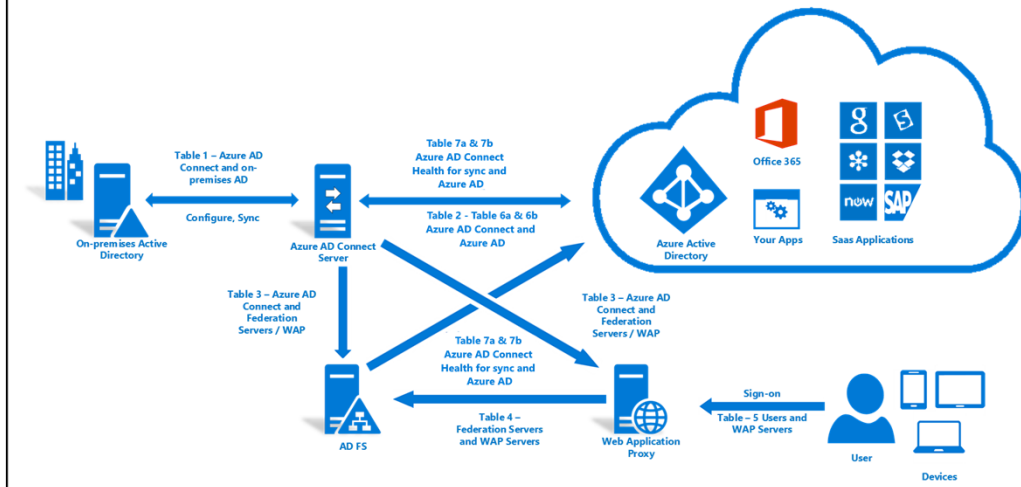




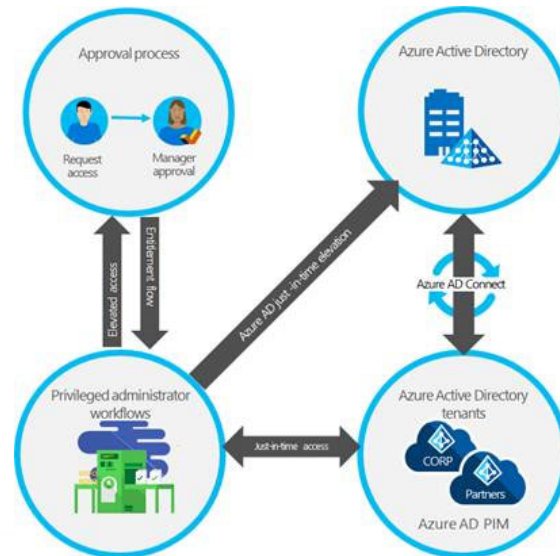




Hybrid Identity Required Ports and Protocols



Azure AD PIM



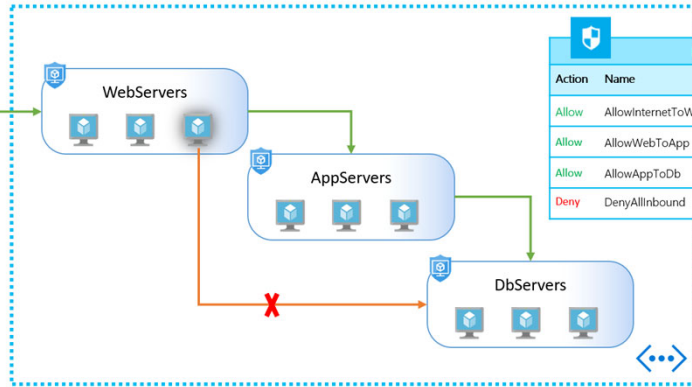


Implement Platform Protection

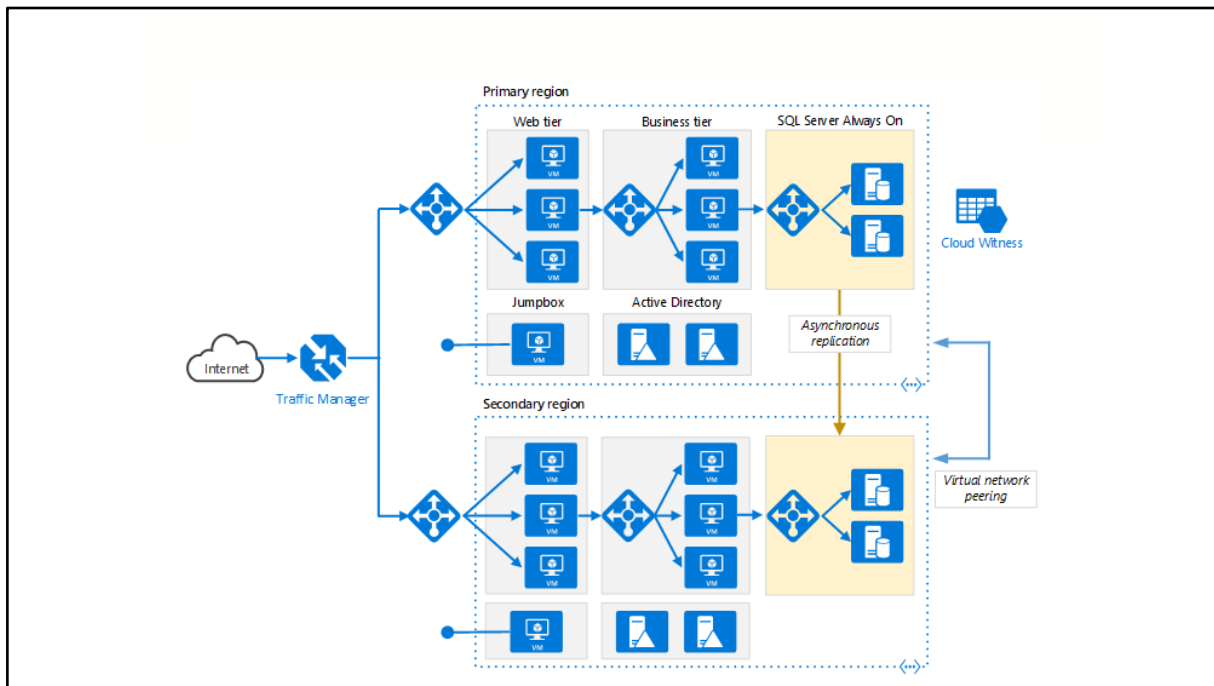
NSGs and ASGs

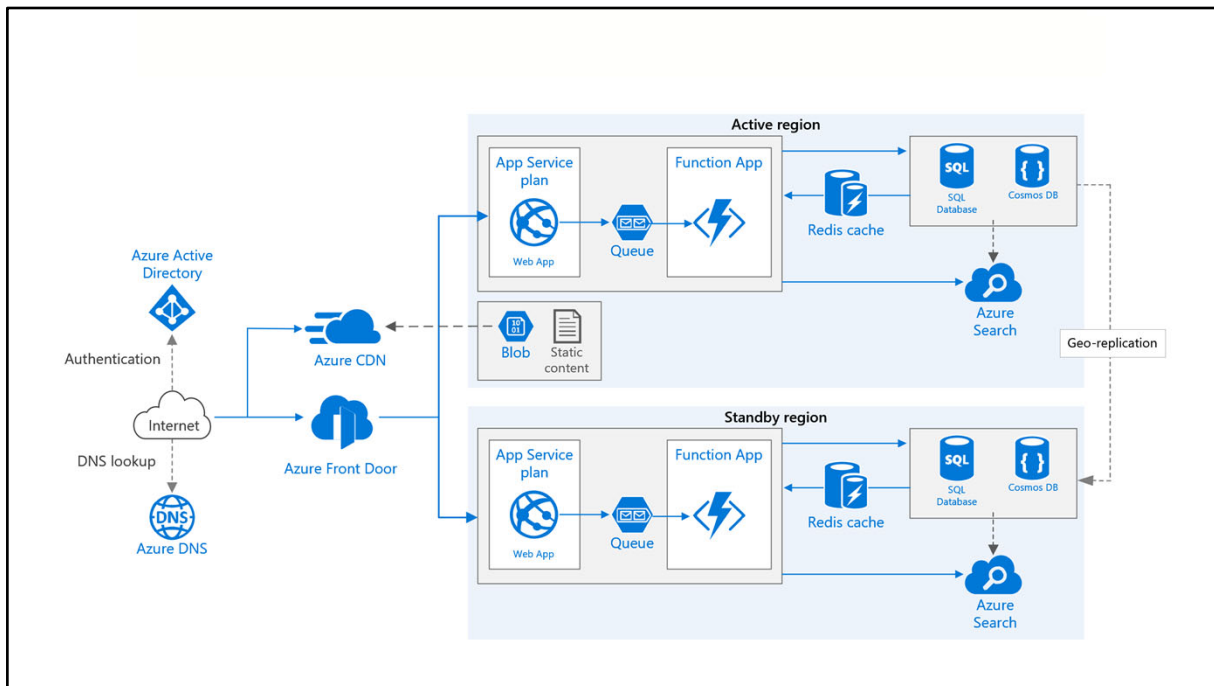


Internet

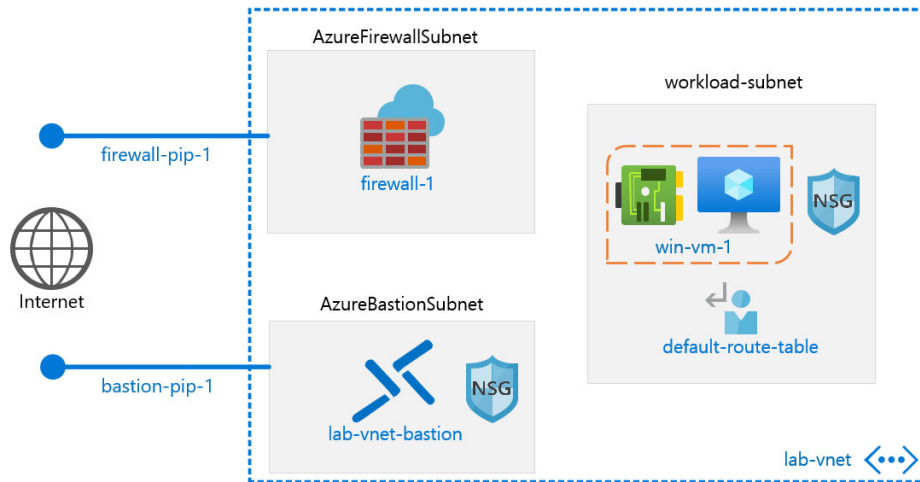


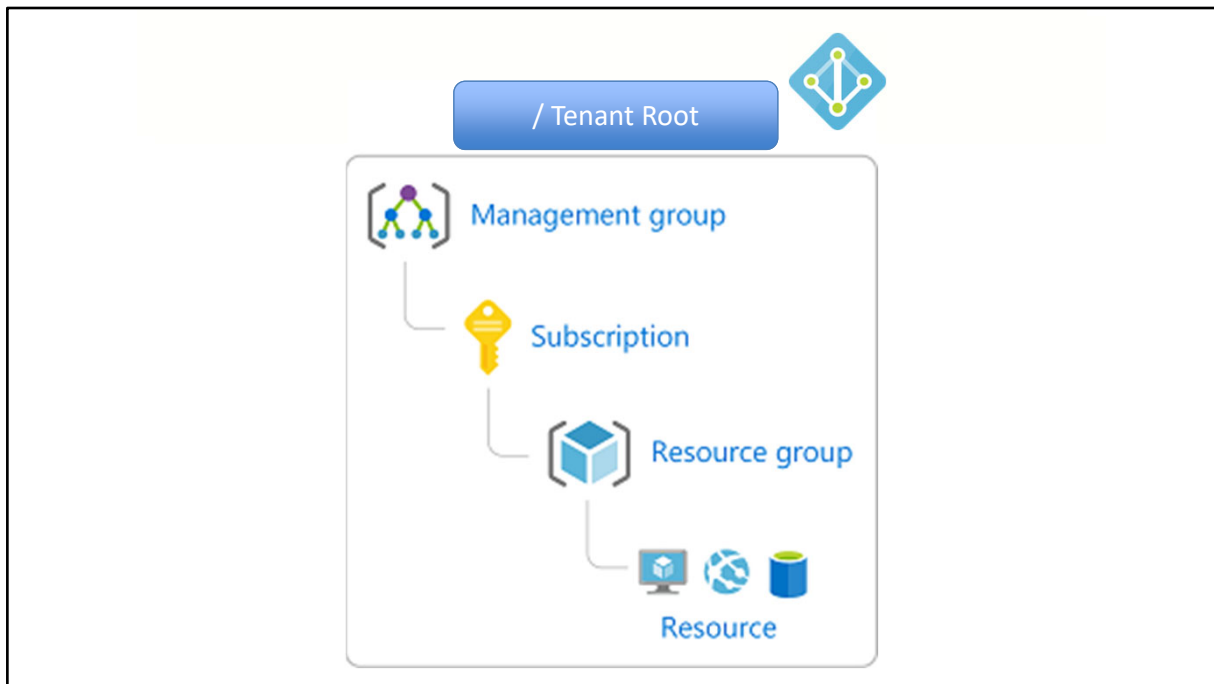
Network Security Group (NSG)				
Action	Name	Source	Destination	Port
Allow	AllowInternetToWeb	Internet	WebServers	80,443 (HTTP/HTTPS)
Allow	AllowWebToApp	WebServers	AppServers	443 (HTTPS)
Allow	AllowAppToDb	AppServers	DbServers	1443 (MySQL)
Deny	DenyAllInbound	Any	Any	Any



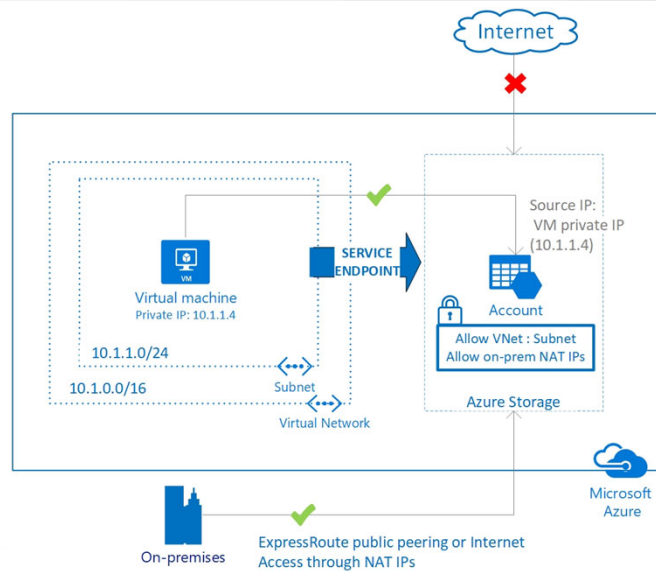


Azure Firewall

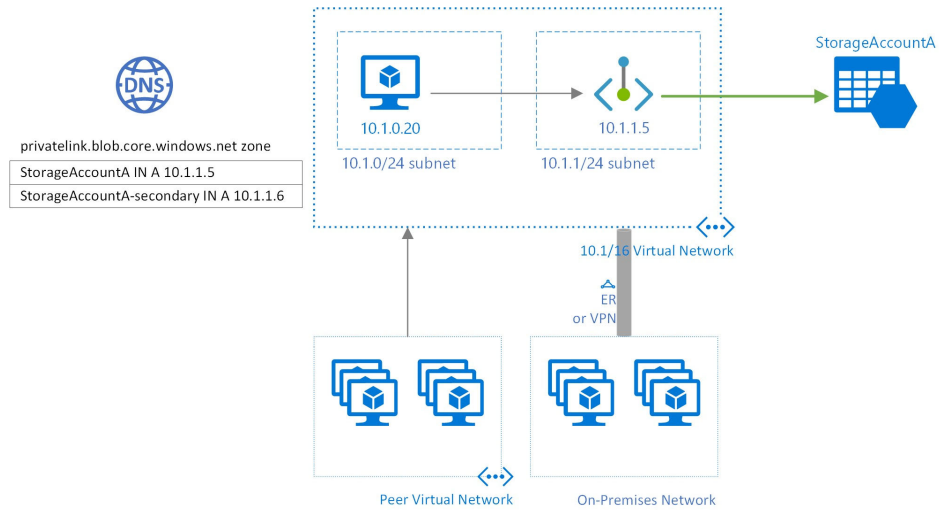




Service endpoints



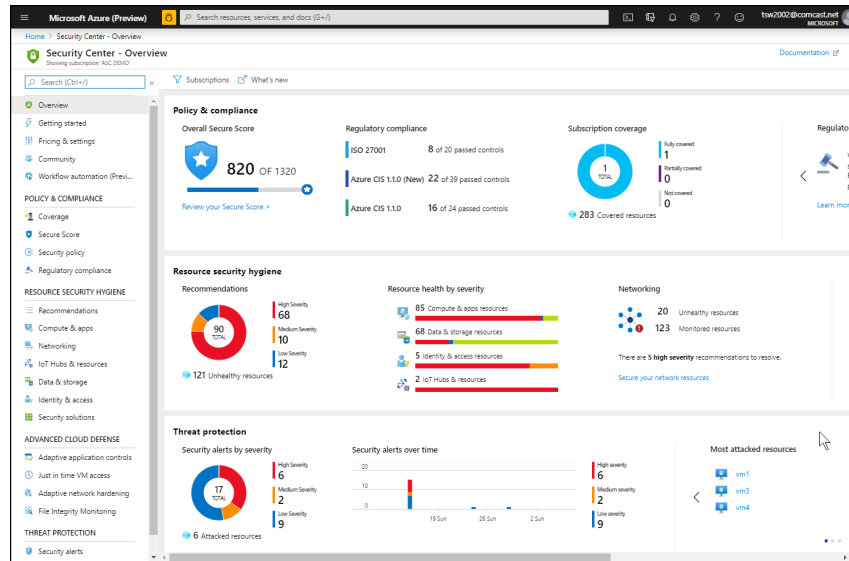
Private endpoints





Manage Security Operations

Azure Security Center



Azure Sentinel

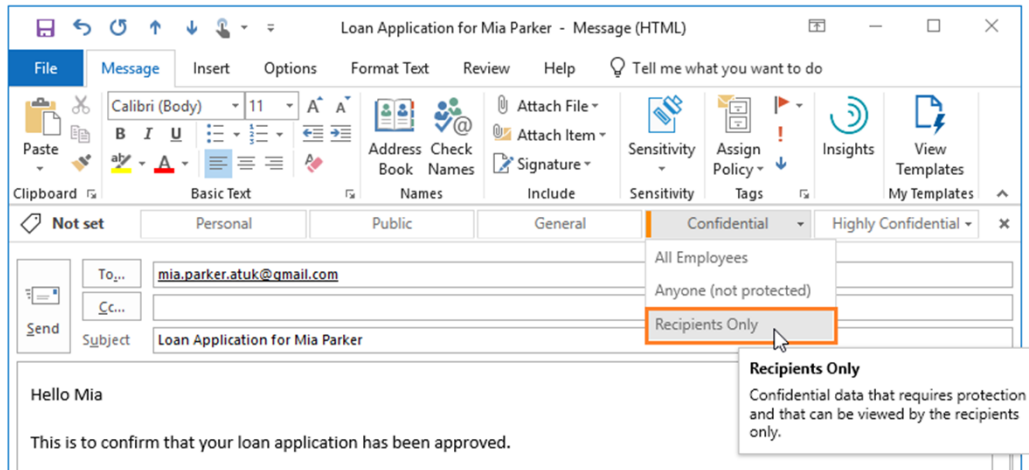
The screenshot displays the 'Azure Sentinel - Data connectors' page in the Microsoft Azure portal. The page is divided into several sections:

- Header:** Microsoft Azure (Preview) and a search bar.
- Left Sidebar:** Navigation menu with options: General (Overview, Logs, News & guides), Threat management (Incidents, Workbooks, Hunting, Notebooks), Configuration (Data connectors, Analytics, Playbooks, Community, Settings).
- Main Content Area:**
 - Connectors Summary:** 32 Connectors, 1 Connected, 1 Coming soon.
 - Search:** Search by name or provider. Filters: PROVIDERS: All, DATA TYPES: All.
 - Connector List:** A table listing various connectors, including Amazon Web Services, Azure Active Directory, Azure Active Directory Identity Protection, Azure Activity, Azure Advanced Threat Protection (Preview), Azure Information Protection (Preview), Azure Security Center, Barracuda CloudGen Firewall, Barracuda Web Application Firewall, and Check Point.
 - Amazon Web Services Detail Panel:**
 - Status:** Not connected.
 - Description:** Follow these instructions to connect to AWS and stream your CloudTrail logs into Azure Sentinel.
 - Last data received:** --
 - Related content:** 2 Workbooks, 2 Queries.
 - Data received:** A line graph showing data received over time, with a peak around January 20th.
 - Buttons:** Open connector page.

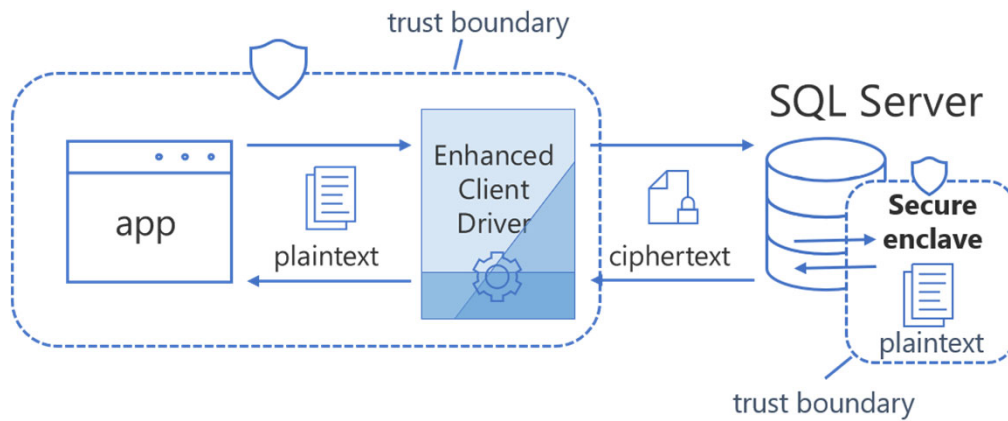



Secure Data and Applications

Azure Information Protection




Always Encrypted





Exam AZ-500 Item Types

 Pearson

⬆️

Question 4 (of 5)

☐ Review later

☐ Comment later

Time remaining 01:58:22

Your network contains an Active Directory domain named contoso.com. The domain contains two servers named Server1 and Server2 that run Windows Server 2012 R2. Server1 has the Group Policy Management feature installed. Server2 has the Print and Document Services server role installed.

On Server2, you open **Print Management** and you deploy a printer named Printer1 by using a Group Policy object (GPO) named GPO1.

When you open GPO1 on Server1, you discover that the Deployed Printers node does not appear.

You need to view the Deployed Printers node in GPO1.

What should you do?

- ☐ A. On Server1, add and share a printer.
- ☐ B. On Server1, install the Print and Document Services Tools.
- ☐ C. On a domain controller, create a Group Policy central store.
- ☐ D. On Server1, modify the Group Policy filtering options of GPO1.

?

Help

📊

Calculator

🖥️

Color scheme

↺️

Reset

⬅️

Previous

➡️

Next



Question 2 (of 9)

Time remaining 01:45:43

- ☐ Review later
- ☐ Comment later

You are an administrator for fabrikam.com.

You need to prove domain ownership for your domain for Office 365.

Which two DNS record types can you create? Each correct answer presents a complete solution.

- ☐ A. Host record (A)
- ☐ B. Text record (TXT)
- ☐ C. Service record (SRV)
- ☐ D. Alias record (CNAME)
- ☐ E. Mail Exchanger record (MX)



Help



Calculator



Color scheme



Reset



Previous



Next

You need to move an Azure VM to another hardware host.

Solution: You redeploy the VM.

Does this solution meet the goal?

- a. Yes
- b. No

You need to move an Azure VM to another hardware host.

Solution: You enable boot diagnostics.

Does this solution meet the goal?

- a. Yes
- b. No

Question 5 (of 9)

Review later

Comment later

Time remaining 01:38:28

You have a Microsoft SharePoint 2013 Service Pack 1 (SP1) server farm.

You need to recommend which tools should be used to recover deleted SharePoint site groups, deleted document libraries, and deleted SharePoint Designer 2010 workflows. The solution must use the minimum amount of administrative effort.

Which tool should you recommend for each type of content? To answer, drag the appropriate tool to the correct recovery task. Each tool may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

Tool

Microsoft SQL Server backups

Recycle Bin

Windows Server Backups

Recovery Task

Document libraries

SharePoint Site groups

SharePoint Designer workflows

Microsoft SQL Server backups

Recycle Bin

Resources

?

Help

Calculator

Color scheme

Reset

Previous

Next

38

Question 4 (of 5)

Review later

Comment later

Time remaining 01:56:12

You have a Hyper-V host named Server1.

A technician creates a virtual machine named VM1 on Server1 by using the New Virtual Machine Wizard.

You start VM1 and you discover that there is no option to start by using PXE.

You need to ensure that you can start VM1 by using PXE.

Which three actions should you perform in sequence? (To answer, move the appropriate three actions from the list of actions to the answer area and arrange them in the correct order.)

Actions

Shut down VM1.

Modify the BIOS settings of VM1.

Enable DHCP guard on the legacy network adapter.

Answer Area

1

Modify the virtual switch settings of the legacy network adapter.

2

Add a legacy network adapter to VM1.

3

Install Integration Services on VM1.

?

Help

Calculator

Color scheme

Reset

Previous

Next

39

Question 18 of 32

You configure a SharePoint Server 2010 Service Pack 1 (SP1) server farm.

You need to enable the cache profile for anonymous users on internal collaboration sites for the site collection. You also need to allow administrators to choose a different page output cache profile for page layouts.

What should you do? (To answer, configure the appropriate option or options in the dialog box in the answer area.)

Answer Area

Libraries Site Pages Shared Documents	Output Cache Select the Enable output cache check box to enable output caching in this site collection.	<input checked="" type="checkbox"/> Enable output cache
Lists Calendar Tasks	Default Page Output Cache Profile A cache profile specifies how long items should be held in the cache. It also describes to the caching system how to determine whether a cached page element is in fact valid for other requests for the same element from different users. You can specify different cache profiles to use for anonymous and authenticated users. This optimizes the use of the cache based on the authentication methods allowed on the site. Page output cache profiles specifically affect portal publishing pages. Learn more about the default page output cache profile.	Anonymous Cache Profile <div>intranet (Collaboration Site)</div> Optimized for collaboration sites where authoring, web part customization, and minor version are enabled.
Discussions Team Discussion		Authenticated Cache Profile <div>Disabled</div> Caching is not enabled
Recycle Bin	<div>Reset(T) Instructions(I)</div>	

Case Study

Time remaining 01:56:02

Question

Background

Existing Environment

Business Requirements

Technical Requirements

Problem Statements

Exhibits

This exam includes at least one case study. **Case studies are not timed separately. You can use as much exam time as you would like to complete each case.** However, there may be additional case studies and sections on this exam. You must manage your time to ensure that you are able to complete all questions included on this exam in the time provided.

To answer the questions included in a case study, you will need to reference information that is provided in the case study. Case studies might contain exhibits and other resources that provide more information about the scenario that is described in the case study. Each question is independent of the other questions in this case study.

At the end of this case study, a review screen will appear. This screen allows you to review your answers and to make changes before you move to the next section of the exam. After you begin a new section, you cannot return to this section.

To start the case study

To display the first question in this case study, click the **Next** button. Use the buttons in the left pane to explore the content of the case study before you answer the questions. Clicking these buttons displays information such as business requirements, existing environment, and problem statements. If the case study has an **All Information** tab, note that the information displayed is identical to the information displayed on the subsequent tabs. When you are ready to answer a question, click the **Question** button to return to the question.

?

?

?

?

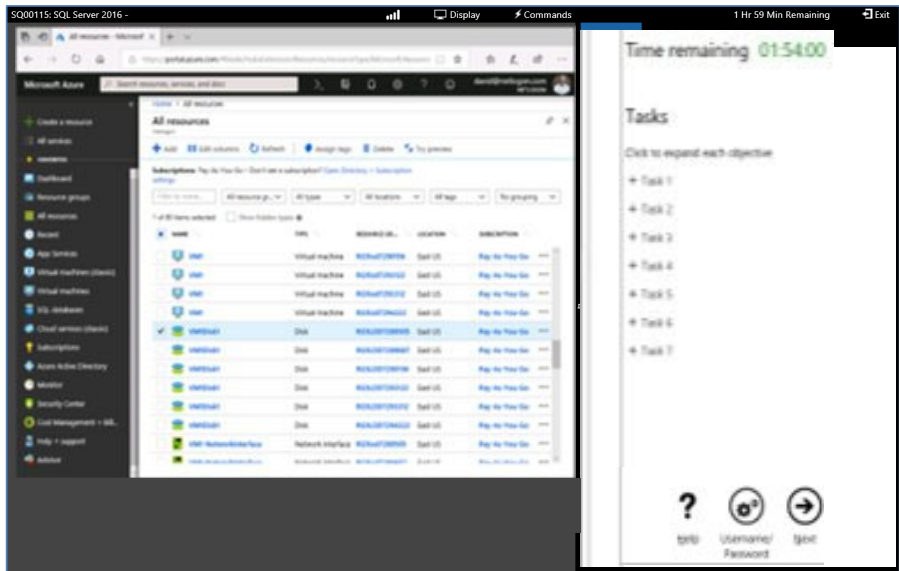
Help

Calculator

Color scheme

Reset

Next



A large, light gray play button icon with a white triangle pointing right, centered within a circle. The circle has a subtle drop shadow.

Microsoft Online Testing

 Pearson

Microsoft Online Testing Process

Select Exam Delivery Option

For: VUE-PCA: VUE Demo

All fields are required.

How do you want to take your exam? [Exam delivery option descriptions](#)

☐ At a local test center

☒ At my home or office

☐ I have a Private Access Code

Microsoft Online Testing Process

Select Date
[Why can't I find an available appointment?](#)

< April 2020 >

Su	Mo	Tu	We	Th	Fr	Sa
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30		

Select a date from the calendar. Only available dates can be selected.

Available start times: Wednesday, April 1, 2020
Times shown in: America/Chicago-CDT [Change](#) | [Show 24-hour](#)

Morning Afternoon

12:00 AM 12:00 PM

Microsoft Online Testing Process

Start Exam

1

Click on the "Copy Access Code" button below. This will automatically enter your access code into OnVUE once it is running. This access code will authorize you to start the exam check-in process.

123-456-789


Copy Access Code

2

Click "Download". Once complete, run the OnVUE application from the downloads folder.
Alert! Mac users, if prompted, will need to allow OnVUE within their 'System Preferences: Security & Privacy: Privacy' settings for Microphone, Camera, Automation, and Input Monitoring.

Download

以下の日本語の説明は、ここをクリックするか、下にスクロールしてください



Enter your unique exam access code and phone number

1. Your access code may have been entered for you

123-456-789

If you do not see the access code, you will need to manually enter it. You can find your access code on the exam launch page.

2. Enter phone number

+1

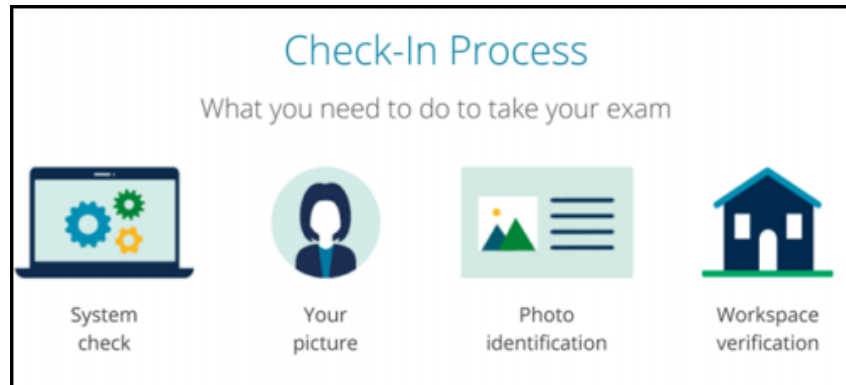
555-555-5555

Enter a phone number with country code, example U.S. +1; we will contact you if there's an issue with check-in or exam delivery.

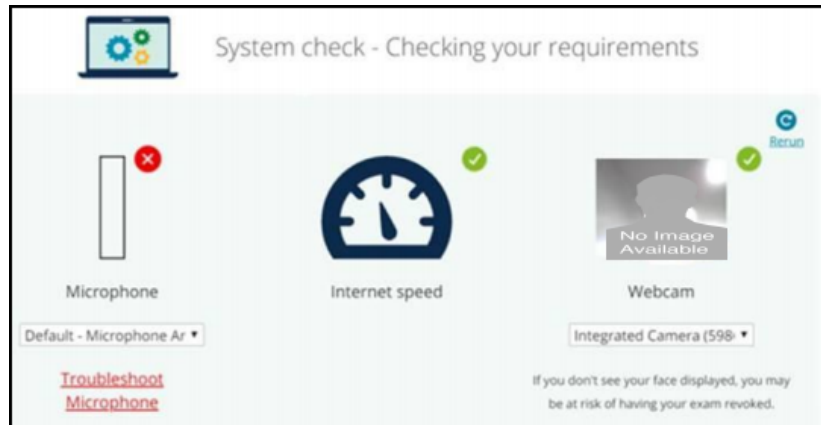
☐ I do not have a phone available at this time.



Microsoft Online Testing Process



Microsoft Online Testing Process



Microsoft Online Testing Process

Use your mobile phone to take your required verification photos



1. Select access method

- ☐ Text message
- ☐ Type URL into mobile phone

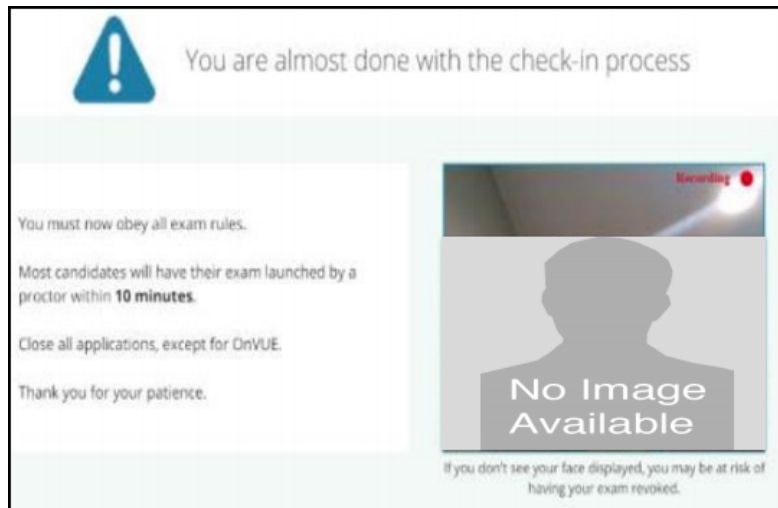
2. Enter contact information

If you don't have a mobile phone, [use our webcam](#) to take the required photos.

Verification options:

- Your picture
- Photo identification
- Workspace verification

Microsoft Online Testing Process



AZ-500 Exam Strategy

- Focus your skills accordingly:
 - 60 percent Azure portal
 - 20 percent Azure PowerShell
 - 10 percent Azure CLI
 - 10 percent KQL
- Azure AD PIM all day long
- Expect performance-based labs, but be happy if you don't see 'em

Thank you!

- Course materials: timw.info/az500
- Twitter: [@TechTrainerTim](https://twitter.com/TechTrainerTim)
- Work: timw.info/ps
- Web: timw.info

