Question #1 *Topic 1*

Which two integrations require the VMware Identity Manager Connector component? (Choose two.)

A. VMware Horizon

B. Email Relay

C. Certificate Services

D. RADIUS Auth Adapter

E. Syslog

Suggested Answer: *AE*
Reference:
https://docs.vmware.com/en/VMware-Identity-Manager/3.1/vidm-install/GUID-881783AC-887F-436F-9A8F-F22B911C47E6.html
https://docs.vmware.com/en/VMware-Identity-Manager/services/identitymanager-connector-win/GUID-F3FD79B6-5F9F-4330-95F3-AF163A5D19C4.html

b33droid 4 years, 2 months ago
As mentionned A and D are correct
About syslog, it's only when you need to setup an external syslog server
https://docs.vmware.com/en/VMware-Workspace-ONE-Access/20.01/workspace_one_access_install/GUID-A775924D-EF56-4C9F-95C0-AFFC7F40555D.html
upvoted 1 times

gabrielramos 4 years, 2 months ago
Correct Answer is A, D.

https://docs.vmware.com/en/VMware-Workspace-ONE-Access/19.03/identitymanager-connector-win/GUID-F3FD79B6-5F9F-4330-95F3-AF163A5D19C4.html
upvoted 2 times

stjwh1 4 years, 5 months ago
I think A,D
upvoted 2 times

Question #2 *Topic 1*

Which function processes device information and applies actions automatically based on configurations created by an administrator?

A. Admin Reports

B. Conditional Access

C. Compliance Policy

D. Device Profile

Suggested Answer: *D*

gabrielramos 4 years, 2 months ago

Confirm Correct Answer is D:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1909/UEM_Managing_Devices/GUID-AWT-DEVICEPROFILESOVERVIEW.html

upvoted 1 times

gabrielramos 4 years, 2 months ago

I noticed that it can be Compliance Policy.

The compliance engine is an automated tool by Workspace ONE UEM powered by AirWatch that ensures all devices abide by policies that you define. These policies can include basic security settings such as requiring a passcode and enforcing certain precautions including passcode strength, blacklisting certain apps, and requiring device check-in intervals.

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/UEM_Managing_Devices/GUID-AWT-COMPLIANCEPOLICIESOVERVIEW.html

upvoted 1 times

Question #3 *Topic 1*

Which policy should an administrator modify to grant a user access to the company's federated Web app in Workspace ONE?

A. Default access policy set

B. Default compliance policy

C. Default authentication user

D. Default profile policy

Suggested Answer: *A*
Reference:
https://pubs.vmware.com/workspace-portal-21/topic/com.vmware.ICbase/PDF/workspace-portal-21-administrator.pdf

Lance_D 4 years, 2 months ago

A is correct answer

upvoted 2 times

gabrielramos 4 years, 2 months ago

Confirm Correct Answer is A:

https://docs.vmware.com/en/VMware-Workspace-ONE-Access/19.03/idm-administrator/GUID-ECA63317-D7FD-4CE3-94FC-1BEADC8D9792.html

upvoted 2 times

Question #4 *Topic 1*

For a hybrid SaaS customer, what Workspace ONE components would always need to be installed On-premises? (Choose two.)

A. VMware Identity Manager

B. VMware Unified Access Gateway

C. VMware Email Notification Service v2

D. VMware AirWatch Cloud Messaging

E. VMware Tunnel

Suggested Answer: *AD*
Reference:
https://techzone.vmware.com/sites/default/files/resource/vmware_workspace_one_reference_architecture_for_saas_deployments.pdf

gabrielramos 4 years, 2 months ago

Confirm Correct Answer is A, D:

https://techzone.vmware.com/blog/updated-vmware-workspace-one-reference-architecture-saas-deployments

upvoted 1 times

daigoking 4 years, 2 months ago

You can implement VMware Identity Manager using on-premises or SaaS-based implementation models. No necessary always need to be on-premises.
So answer should be B, E

https://techzone.vmware.com/sites/default/files/resource/vmware_workspace_one_reference_architecture_for_saas_deployments.pdf

upvoted 2 times

gabrielramos 4 years, 2 months ago

I agree. I miss understood the question. As the messaging components are in inside the cloud components and vIDM is deployed in cloud in a SaaS deployments, the only options are the Connectors or Gateways. In this case B and E! Thank you!

upvoted 2 times

Ossama_369 4 years, 4 months ago

its B.E

upvoted 1 times

gabrielramos 4 years, 2 months ago

The UAG and VMware Tunnel are optional components. Otherwise, Airwatch and IDM Gateways are must do if you want to connect to SaaS Workspace Environment.

upvoted 1 times

stjwh1 4 years, 4 months ago

I think B,E

upvoted 1 times

gabrielramos 4 years, 2 months ago

The UAG and VMware Tunnel are optional components. Otherwise, Airwatch and IDM Gateways are must do if you want to connect to SaaS Workspace Environment.

upvoted 1 times

Question #5 *Topic 1*

Which component is required to integrate Workspace ONE Intelligence into a Workspace ONE solution for enhanced endpoint and application management?

A. Horizon Connection Server

B. Workspace ONE Intelligence Connector

C. Cloud Connector

D. Workspace ONE IDM Connector

Suggested Answer: *C*

Agalliasis 3 years, 11 months ago

Answer is B.
https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligence-documentation/GUID-04_intel_reqs.html

upvoted 1 times

gabrielramos 4 years, 2 months ago

Correct Answer is B:

https://docs.vmware.com/en/VMware-Workspace-ONE/services/Intelligence/GUID-AWT-CUSTOMREPORTS-REQUIREMENTS.html

upvoted 1 times

telouat 4 years, 3 months ago

B
https://docs.vmware.com/en/VMware-Workspace-ONE/services/Intelligence/GUID-AWT-CUSTOMREPORTS-REQUIREMENTS.html

upvoted 1 times

JorgeLopez 4 years, 4 months ago

https://www.vmware.com/content/dam/digitalmarketing/vmware/es/pdf/products/workspace-one/vmware-workspace-one-intelligence-faq.pdf

It's B

upvoted 1 times

stjwh1 4 years, 4 months ago

I" choose B

upvoted 2 times

Question #6 *Topic 1*

Which are the key functionalities of Workspace ONE Intelligence? (Choose three.)

A. Content Insights

B. App Analytics

C. Mobile Analytics

D. Powerful Automation

E. Email Automation

F. Integrated Insights

Suggested Answer: *BDF*
Reference:
https://www.vmware.com/products/workspace-one/intelligence.html

gabrielramos 4 years, 2 months ago

Confirm Correct Answer B, D, F:

https://www.vmware.com/products/workspace-one/intelligence.html

upvoted 1 times

Question #7 *Topic 1*

Which three features can be enabled by integrating Workspace ONE UEM and VMware Identity Manager services? (Choose three.)

A. Unified Catalog

B. Mobile Application Management

C. Mobile Email Management

D. Password (Airwatch Connector)

E. Single Sign-On to web applications

F. Compliance Auth Adapter

Suggested Answer: *DEF*

danish 4 years, 2 months ago

It should be ADF.
IT is single sign on for web apps not native apps

upvoted 1 times

gabrielramos 4 years, 2 months ago

Correct Answer is A, E, F:

https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1-IDM-deploymentguide/GUID-F072888F-FC6F-4A6B-9574-2CAAE7E96A85.html

upvoted 1 times

telouat 4 years, 3 months ago

ADF
https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1-IDM-deploymentguide/GUID-F072888F-FC6F-4A6B-9574-2CAAE7E96A85.html

upvoted 1 times

gabrielramos 4 years, 2 months ago

"D" depends on Airwatch Cloud Connector deployment

upvoted 1 times

OzMike 4 years, 4 months ago

A, D, E

upvoted 1 times

gabrielramos 4 years, 2 months ago

"D" depends on Airwatch Cloud Connector deployment

upvoted 1 times

nick_name 4 years, 4 months ago

A,E,F https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1-IDM-deploymentguide/GUID-EF834B6D-C3EC-48BA-B38D-1574F7E4B773.html

upvoted 1 times

Question #8 *Topic 1*

When configuring profiles in the Workspace ONE UEM Console for Android devices, why would some setting features and payloads be supported for specific original equipment manufacturers (OEMS) and/or operating system (OS) versions?

A. Profile configuration requires a device directly purchased from Google

B. Profile configuration requires an application built with the AirWatch SDK installed on the device

C. Profile configuration is dependent on operating system and firmware API availability

D. Profile configuration is XML-based and depending on the OEM or OS, the device may not support XML

Suggested Answer: *C*

Lance_D 4 years, 2 months ago

C is correct answer - confirmed

upvoted 1 times

Mayurgadge580 4 years, 2 months ago

Correct answer is B

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1810/vmware-airwatch-android-(legacy)-platform-guide.pdf

For application integration, you can
integrate any of your existing enterprise apps with the AirWatch Software Development Kit (SDK) to enhance their functionality.

upvoted 1 times

gabrielramos 4 years, 2 months ago

Confirm Correct Answaer is C:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2001/Android_Platform/GUID-AWT-SETUP-CONCEPT.html

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2001/Android_Platform/GUID-AWT-REQUIREMENTSFORDEPLOYINGANDROIDFORWORK.html

upvoted 1 times

Question #9 *Topic 1*

Which Unified Access Gateway (UAG) component can use an AirWatch generated certificate for Inbound SSL traffic?

A. VMware Tunnel

B. Content Gateway

C. AirWatch Cloud Connector

D. VMware Secure Email Gateway

Suggested Answer: *B*

Reference:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/9.7/content-gateway-to-unified-access-gateway-migration-guide.pdf

gabrielramos Highly Voted 4 years, 2 months ago

Correct answer is A:

Devices are authenticated to the Tunnel Proxy with a certificate issued via the SDK as configured in the AirWatch Admin Console.
https://docs.vmware.com/en/Unified-Access-Gateway/3.2.1/com.vmware.uag-321-deploy-config.doc/GUID-8B96F385-ADE5-4502-8485-6269EE41D222.html

AirWatch generates a unique identity certificate pair for both the AirWatch and VMware Tunnel environments.
https://resources.workspaceone.com/view/yr8n5s2b9d6qqbcfjbrw/en

upvoted 5 times

Question #10 *Topic 1*

Which is required to suppress the Apple Enrollment Terms of Use (TOU) for agreement prior to iOS device management?

A. Configure Apple VPP

B. Configure DEP

C. Configure pre-registration TOU

D. Configure post-registration TOU

Suggested Answer: *A*

Lance_D 4 years, 2 months ago

B is correct

upvoted 2 times

gabrielramos 4 years, 2 months ago

Correct Answer is B:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2001/AppleBusinessManager/GUID-AWT-C-INTEGRATEWITHDEP.html

You can automatically register new Apple Devices with DEP.

upvoted 2 times

OzMike 4 years, 4 months ago

B.) DEP

upvoted 2 times

nick_name 4 years, 4 months ago

the answer is B. VVP is for volume Purchase

upvoted 3 times

stjwh1 4 years, 4 months ago

I'll choose B

upvoted 4 times

Question #11 *Topic 1*

Which two paths can you take to upload a SSL Certificate for VMware AirWatch Secure Email Gateway (SEG) V2? (Choose two.)

A. Uploading the SSL Certificate through SEG V2 Installer

B. Uploading the SSL Certificate to IIS on the SEG V2 server

C. Uploading the SSL Certificate to VMware Unified Access Gateway Edge Service configuration

D. Uploading the SSL Certificate in the Workspace ONE UEM Console

E. Copying/Pasting the SSL Certificate to the SEG V2 server

Suggested Answer: *AB*

gabrielramos 4 years, 2 months ago

Correct Answer is A, D:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1-Secure-Email-Gateway/GUID-D71CBEF1-3754-4362-95EE-15B269E68B61.html

upvoted 2 times

stjwh1 4 years, 4 months ago

I'll choose A,D

upvoted 1 times

Question #12 *Topic 1*

What Workspace ONE process allows an administrator to prepare 50 newly purchased Windows 10 devices for enrollment without connectivity to the Internet and without using Workspace ONE Intelligent Hub installation parameters?

A. Windows Auto-Discovery

B. Command Line staging

C. Manual staging

D. Azure AD Integration enrollment

Suggested Answer: *A*
Reference:
https://techzone.vmware.com/troubleshooting-windows-10-vmware-workspace-one-operational-tutorial#968027

Benson760207Tseng 4 years, 2 months ago
Hi All, this question will be changed from "50 newly purchased Windows 10" to "Small newly purchased Windows 10", so this answer is "A"?
upvoted 2 times

Mayurgadge580 4 years, 2 months ago
Windows Auto-Discovery is an optional method of enrolling devices that only requires the end-user's email address to begin the enrollment process
upvoted 2 times

gabrielramos 4 years, 2 months ago
Confirm Correct Answer A:

https://docs.vmware.com/en/VMware-Workspace-ONE/services/intelligent-hub_IDM/GUID-24C5839F-598A-4508-9500-A058D3955AF9.html

https://techzone.vmware.com/troubleshooting-windows-10-vmware-workspace-one-operational-tutorial#968027
upvoted 4 times

Question #13 *Topic 1*

Workspace ONE VMware Tunnel supports which X.509 certificate file format?

A. .pfx

B. .p7s

C. .pem

D. .p12

Suggested Answer: *A*

Zub1 1 year, 6 months ago

Workspace ONE VMware Tunnel supports X.509 certificate file format in .pem format.

A PEM file is a container format for certificates and keys that are encoded using base64. This format is widely used for SSL/TLS certificates and private keys, and it is supported by many web servers, including Apache and Nginx.

When configuring VMware Tunnel, the PEM format certificate can be uploaded to the Workspace ONE UEM Console, and then pushed to the devices during the Tunnel configuration. The certificate can be generated using a certificate authority (CA) or self-signed using OpenSSL or similar tools.

In summary, Workspace ONE VMware Tunnel supports X.509 certificates in the PEM file format, which is a widely used format for certificates and keys.

upvoted 1 times

gabrielramos 4 years, 2 months ago

According the documentation it could be either .pfx or .p12.

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2001/Tunnel_Linux/GUID-A41D8AAC-BA17-40DD-975A-A17126ECBAC3.html

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Tunnel_Linux/GUID-AWT-CONFIGURELNX.html

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1907/Tunnel_Linux/GUID-AWT-CONFIGURESSLCERTROTATION.html

upvoted 2 times

Question #14 *Topic 1*

Which two settings need to be configured to allow a user to move content from Admin Repository A to Admin Repository B in the VMware Content Locker?
(Choose two.)

A. Admin Repository A needs Allow Savings to Other Repositories enabled

B. Local storage needs to be enabled for VMware Content Locker

C. Admin Repository B needs Write enabled

D. Admin Repository A needs Allow Edit Enabled

E. Sharing needs to be enabled in the SDK setting for VMware Content Locker

Suggested Answer: *DE*

Zub1 1 year, 6 months ago

The correct answer is:

C. Admin Repository B needs Write enabled
D. Admin Repository A needs Allow Edit Enabled

To allow a user to move content from Admin Repository A to Admin Repository B in the VMware Content Locker, Admin Repository A should have "Allow Edit" enabled and Admin Repository B should have "Write" permission enabled.

The "Allow Edit" permission allows users to edit or move content stored in Admin Repository A. The "Write" permission enables users to write to and store content in Admin Repository B.

Option A (Allow Savings to Other Repositories) and option E (Sharing enabled in SDK setting) are not relevant to the process of moving content between repositories in VMware Content Locker.

Option B (Local storage enabled) is also not required to move content between repositories but may impact the user's ability to access and manage content in the Content Locker app.

upvoted 1 times

Benson760207Tseng 4 years, 2 months ago

Hi All, this question will be changed, C "Admin Repository B needs Write enabled" change to "Admin Repository B needs Allow Edit Enabled", so this answer is "CD"?

upvoted 1 times

b33droid 4 years, 1 month ago

From the current documentation Last Updated 05/20/2020, the wording is still "Allow Write".
https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/MCM/GUID-AWT-REPO-CFS-SYNC.html?hWord=N4IghgNiBc4CYFsCWA7ABAJwKYAcD2AzkgC54YCeIAvkA

upvoted 1 times

b33droid 4 years, 1 month ago

Allow Edit This setting only applies to write-enabled repositories.

upvoted 1 times

gabrielramos 4 years, 2 months ago

I would choose C, D, once:

Allow Saving to Other Repository is to save to Personal Content.
Local Storage saves in the local device.
Couldn't find Sharing configuration in SDK settings for VMware Content Locker.

To receive the new content Repository B must be write-enabled and to modify Repository it should be edit-enabled.

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1811/VMware-Workspace-ONE-UEM-Mobile-Content-Management/GUID-AWT-REPO-CFS-SYNC.html

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1811/VMware-Workspace-ONE-UEM-Mobile-Content-Management/GUID-AWT-REPO-DET-CONFIG.html
upvoted 2 times

Question #15 *Topic 1*

A topology, which includes placement of Workspace ONE service applications within layered internal networks, as well as communication workflows of requesting and receiving services, is an example of what kind of architectural design?

A. Conceptual

B. Logical

C. Virtual

D. Physical

Suggested Answer: *B*
Reference:
https://techzone.vmware.com/resource/workspace-one-and-horizon-reference-architecture#sec14-sub3

NKG123 4 years ago

Physical
A lot of guys don't know the right answers. If we have network flows it can only be physical !!!
upvoted 1 times

NKG123 4 years ago

Hhadjdjjdjd
upvoted 1 times

RevanT 4 years, 2 months ago

The answer is B ; Logical.

From the VMware exam prep videos Logical Design includes Product name: Network Location: and Components.
If it were Physical, it would include Communication Flow, Network Ports, and Hardware Requirements.
upvoted 2 times

bryanseesu 4 years, 3 months ago

I would select D.since the question here is mentioning about layered internal networks and requesting and receiving services.
upvoted 1 times

gabrielramos 4 years, 2 months ago

To physical it should mention all the components that compose the solution. For example it would say Airwatch Cloud Conector and Identity Manager Appliance, instead of Workspace One Application services.
upvoted 1 times

Question #16 *Topic 1*

Which two registration modes are available for Android Enterprise endpoints? (Choose two.)

A. Work Profile

B. Work Supervised

C. Work Corporate

D. Work Managed

E. Work Company

Suggested Answer: *rdAC*

Reference:

https://kb.vmtestdrive.com/hc/en-us/articles/360001306414-Android-BYO-Device-Management-

Zub1 1 year, 6 months ago

A: Work Profile

D: Work Managed

upvoted 1 times

Rabbah_Adel_Ammar 4 years, 4 months ago

A and D

upvoted 1 times

OzMike 4 years, 4 months ago

A: Work Profile

D: Work Managed

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2001/Android_Platform/GUID-AWT-AFWDEVICEMODES.html

upvoted 2 times

Question #17 *Topic 1*

When using Okta as a 3 -
Party IdP with Workspace ONE, which party owns the entitlement of resources in Workspace ONE?

A. Workspace ONE

B. Okta

C. SAML

D. OAuth

Suggested Answer: *B*

Zub1 1 year, 6 months ago

When using Okta as a third-party IdP with Workspace ONE, the entitlement of resources in Workspace ONE is owned by Workspace ONE.

Okta serves as the identity provider for Workspace ONE, authenticating users and providing identity information to Workspace ONE. However, the Workspace ONE administrator is responsible for defining and managing user access to resources within the Workspace ONE environment. This includes managing user authentication and authorization, assigning users to specific groups, and configuring policies and access controls based on user roles or other criteria.

Therefore, the correct answer is A. Workspace ONE.

upvoted 1 times

gabrielramos 4 years, 2 months ago

Confirm correct answer B:

https://docs.vmware.com/en/VMware-Workspace-ONE/services/workspaceone_okta_integration/GUID-3CA49953-A8F6-491D-90DF-63588EFC3292.html

upvoted 2 times

Question #18 *Topic 1*

Which two email management technologies allow you to enforce data loss prevention? (Choose two.)

A. PowerShell Integration

B. Secure Email Gateway

C. Direct Google Sync Integration

D. VMware Workspace ONE Boxer

E. Conditional Access

Suggested Answer: *DE*

Zub1 1 year, 6 months ago

The two email management technologies that allow you to enforce data loss prevention are:

B. Secure Email Gateway: This technology provides advanced threat detection, filtering, and response capabilities to protect email communications and enforce data loss prevention policies.

E. Conditional Access: This technology provides policy-based access control to email and other corporate resources based on various criteria, such as user location, device type, and user role. This can help prevent data loss by restricting access to sensitive information on unsecured or non-compliant devices.

Therefore, the correct options are B. Secure Email Gateway and E. Conditional Access.

upvoted 1 times

NKG123 4 years, 1 month ago

Boxer can't be the answer. It's an application. Not email management technology. We're supposed to select A and B. The two methods to configure a SEG.

upvoted 1 times

Lance_D 4 years, 2 months ago

Please see the content in the link below:
https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1811/WS1-PowerShell-Integration.pdf

Email Security Policies for PowerShell IntegrationEmail policies enhance security by restricting email access to non-compliant, unencrypted, inactive, orunmanaged devices. These policies allow you to provide email access to only the required and approveddevices. Email policies also restrict email access based on the device model and the operating systems.These policies are available from Email > Compliance Policies in the UEM console. Activate ordeactivate the policies using the colored buttons under the Active column. Use the edit policy icon underthe Actions column to allow or block a polic

upvoted 2 times

Lance_D 4 years, 2 months ago

Update! I am not so sure of previous comments after reading additional materials. Options B & D may well be correct but again I am not sure. Even my EUC expert contact from vendor struggled with this question

upvoted 1 times

Lance_D 4 years, 2 months ago

A & B is correct - confirmed

Key Design Considerations
VMware recommends using Workspace ONE UEM Secure Email Gateway for all on-premises email infrastructures with deployments of more than 100,000 devices. For smaller deployments or cloud based email, PowerShell is another option.

VMWare Workspace ONE Boxer is a mail client; not a management tool.

upvoted 1 times

gabrielramos 4 years, 2 months ago

Correct Answer B, D:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/WS1-Secure-Email-Gateway/GUID-AWT-SECURINGWITHEMAILPOLICY.html

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/VMware-Workspace-One-Boxer/GUID-AWT-BOXER-EMAIL-SETTINGS.html

upvoted 2 times

⊟ **Rabbah_Adel_Ammar** 4 years, 4 months ago

A and B

upvoted 2 times

⊟ **OzMike** 4 years, 4 months ago

B: SEG

D: Boxer

upvoted 2 times

⊟ **nick_name** 4 years, 4 months ago

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/9.7/vmware-airwatch-guides-97/GUID-AW97-KS_MEM_Email-Infrastructure.html

upvoted 1 times

Question #19 *Topic 1*

A customer has Office 365 that is accessible to all devices for both OWA and Active Sync. The customer wishes to restrict email access so that email is only allowed on Workspace One Managed Devices.
What are two VMware Recommended technologies to achieve this? (Choose two.)

A. VMware Secure Email Gateway

B. VMware Identity Manager

C. AirWatch Cloud Connector

D. VMware Tunnel

E. PowerShell Integration

Suggested Answer: *AE*

Zub1 1 year, 6 months ago
A and B
VMware Identity Manager: VMware Identity Manager is a cloud-based identity management solution that provides single sign-on (SSO) to cloud, mobile, and on-premises applications. It can be used to control access to Office 365 resources and enforce policy-based access control to email and other corporate resources based on various criteria.
upvoted 1 times

Lance_D 4 years, 2 months ago
A and E is correct - but I wonder if this question is another way asking the previous question to confuse exam takers. Denying or permitting access to email is email management task you will use to control DLP. Using email management tools like SEG and PowerShell enable you to do just that- just saying cos this is quite confusing
upvoted 1 times

gabrielramos 4 years, 2 months ago
Confirm correct answer A,E:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2001/WS1_MEM_Guide/GUID-AWT-EMAILPOLICIES.html
upvoted 2 times

Question #20 *Topic 1*

What VMware client application is used for Android Mobile SSO, and what authentication method is utilized by this application?

A. Workspace ONE Web and Certificate Authentication

B. VMware Tunnel and Certificate Authentication

C. Workspace ONE Intelligence Hub and Kerberos

D. VMware Tunnel and Kerberos

Suggested Answer: *A*
Reference:
https://pubs.vmware.com/workspace_one_aw-91/index.jsp?topic=%2Fcom.vmware.aw-vidm-ws1integration-911%2FGUID-1E5128A5-1394-4A50-
8098-947780E38166.html

Zub1 1 year, 6 months ago
A is correct
The VMware client application used for Android Mobile SSO is Workspace ONE Web, and it utilizes Certificate Authentication. Therefore, the correct option is A. Workspace ONE Web and Certificate Authentication.
upvoted 1 times

Lance_D 4 years, 2 months ago
B is correct
https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1_android_sso_config/GUID-1E5128A5-1394-4A50-8098-947780E38166.html
upvoted 1 times

gabrielramos 4 years, 2 months ago
Correct Answer is B:

https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1_android_sso_config/GUID-1E5128A5-1394-4A50-8098-947780E38166.html
upvoted 2 times

bryanseesu 4 years, 3 months ago
The question here is What VMware client application, VMware tunnel is not a client application. I would consider Workspace one Web as a VMware client application.
upvoted 1 times

> **gabrielramos** 4 years, 2 months ago
> But there is a VMware Tunnel App for Android that is a client aplication.
> upvoted 1 times

Rabbah_Adel_Ammar 4 years, 4 months ago
B is Correct
upvoted 3 times

Question #21 *Topic 1*

Which URL would an administrator use to download Unified Access Gateway logs without logging in?

A. https://<virtual appliance domain name>:9443/rest/v1/monitor.7z

B. https://<virtual appliance domain name>:9443/rest/v1/monitor/zip

C. https://<virtual appliance domain name>:9443/rest/v1/monitor/support-archive

D. https://<virtual appliance domain name>:9443/rest/v1/monitor/tar.gz

Suggested Answer: *B*

Zub1 1 year, 6 months ago

The URL that an administrator would use to download Unified Access Gateway logs without logging in is:

https://<virtual appliance domain name>:9443/rest/v1/monitor/support-archive

Therefore, the correct option is C. https://<virtual appliance domain name>:9443/rest/v1/monitor/support-archive.

upvoted 1 times

telouat 4 years, 3 months ago

C

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1907/Tunnel_Linux/GUID-AWT-TUNNELTROUBLESHOOTINGPROXY.html

upvoted 3 times

bryanseesu 4 years, 3 months ago

C is the correct answer:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Tunnel_Linux/GUID-AWT-TUNNELTROUBLESHOOTINGPROXY.html

upvoted 4 times

Rabbah_Adel_Ammar 4 years, 4 months ago

c is correct

upvoted 4 times

Question #22 *Topic 1*

Which Workspace ONE component can be integrated with VMware NSX to implement network micro-segmentation?

A. VMware Tunnel

B. VMware AirWatch Content Gateway

C. VMware Identity Manager Connector

D. VMware AirWatch Secure Email Gateway

Suggested Answer: *A*

Zub1 1 year, 6 months ago

The Workspace ONE component that can be integrated with VMware NSX to implement network micro-segmentation is VMware Identity Manager Connector.

upvoted 1 times

devalk 4 years, 1 month ago

NSX-T is not VMware NSX yet. This is a 3rd party vendor. I think the answer should be C.

upvoted 1 times

gabrielramos 4 years, 2 months ago

Confirm Correct Answer A:

https://techzone.vmware.com/resource/integrating-vmware-tunnel-and-nsx-airwatch-enterprise-mobility-management#section2

upvoted 1 times

Question #23 *Topic 1*

What role does vIDM support in an OpenID Connect (OIDC) authentication flow?

A. Relying Party

B. Resource Server

C. User-Agent

D. OpenID Provider

Suggested Answer: *C*

Zub1 1 year, 6 months ago

D. OpenID Provider.

vIDM (VMware Identity Manager) is an identity management solution that can act as an OpenID Connect (OIDC) provider. As an OIDC provider, vIDM can issue tokens to authenticate users and provide their identity information to relying parties. In an OIDC authentication flow, the OpenID provider is responsible for authenticating the user and issuing an ID token that contains the user's identity information.

upvoted 1 times

gabrielramos 4 years, 2 months ago

For me it's A:

https://docs.vmware.com/en/VMware-Workspace-ONE-Access/20.01/ws1access-resource/GUID-406D8154-3C32-4AD1-A746-619BDF2CCB70.html

upvoted 2 times

Rabbah_Adel_Ammar 4 years, 4 months ago

A is Correct

upvoted 1 times

Question #25 *Topic 1*

What is the VMware recommended practice if you want to apply specific Conditional Access to all your Apple iOS devices regardless of browser or application used on the Apple iOS devices?

A. Create a brand new Access Policy to only contain Apple iOS specific access rules

B. Prioritize Apple iOS platform in Access Policies in the VMware Identity Manager Console

C. Remove other access rules from Access Policies except the Apple iOS access rule

D. Create a custom AirWatch SDK profile and assign it to the Apple iOS devices

Suggested Answer: *D*

Lance_D 4 years, 2 months ago

A is the correct option

upvoted 1 times

gabrielramos 4 years, 2 months ago

Correct Answer is A:

https://docs.vmware.com/en/VMware-Workspace-ONE-Access/20.01/ws1_access_authentication/GUID-C2B03912-C7D8-4524-AE6E-8E8B901B9FD6.html

Access policy by Device Type

upvoted 2 times

Rabbah_Adel_Ammar 4 years, 4 months ago

A is Correct

upvoted 1 times

Question #26 *Topic 1*

An administrator is troubleshooting the Per-App VPN function in the VMware Tunnel and runs the following command: openssl s_client ""showcerts ""connect <TunnelHostname>:8443.

They notice that the response is the certificate from their firewall and not the certificate from the Tunnel server.

What remediation step should be taken?

A. The VMware Tunnel should be re-configured to use the certificate from the firewall

B. The VMware Tunnel SSL traffic needs to pass through the firewall unmodified

C. The VMware Tunnel should be re-configured to trust the certificate from the firewall

D. The VMware Tunnel Certificate should be exported from the console and uploaded to the firewall

Suggested Answer: *C*

gabrielramos 4 years, 2 months ago

Correct Answer is B:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2001/Tunnel_Linux/GUID-AWT-DEPLOYMENT-LOADBALANCE.html

upvoted 1 times

Rabbah_Adel_Ammar 4 years, 4 months ago

B is Correct

upvoted 1 times

Question #27

Topic 1

Users are reporting to IT they are getting an error when attempting to launch mobile apps that require VPN to access.
Which command would an IT Administrator need to run to check the status of the Tunnel Per-App VPN service on the Unified Access Gateway (UAG)?

A. systemctl status pavpn

B. systemctl status vpnd

C. service status vpnd

D. service status pavpn

Suggested Answer: *rdB*

Zub1 1 year, 6 months ago

A. systemctl status pavpn.

To check the status of the Tunnel Per-App VPN service on the Unified Access Gateway (UAG), an IT Administrator would need to run the following command: systemctl status pavpn.

This command will display the current status of the pavpn service, which is responsible for managing the Per-App VPN connections. It will also provide information about any errors or warnings that may be encountered, which can help diagnose any issues that may be preventing users from accessing mobile apps that require VPN.

upvoted 1 times

Lance_D 4 years, 2 months ago

Correct answer is B - confirmed

upvoted 1 times

gabrielramos 4 years, 2 months ago

Correct Answer is B:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/Tunnel_Linux/GUID-AWT-TUNNELTROUBLESHOOTINGPERAPP.html

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/2001/Tunnel_Linux/GUID-8151075D-7C30-42F6-964B-EA5F8630952F.html

upvoted 2 times

bryanseesu 4 years, 3 months ago

Correct Answer is B

upvoted 1 times

nick_name 4 years, 4 months ago

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1909/Tunnel_Linux/GUID-8151075D-7C30-42F6-964B-EA5F8630952F.html

upvoted 3 times

Question #28 *Topic 1*

Which three configuration changes must be made to use an enterprise Certificate Authority (CA) for Mobile SSO with iOS devices? (Choose three.)

A. Integrate 3 party Certificate Authority (CA) with Workspace ONE UEM console

B. Configure Mobile SSO adapters in Workspace ONE to trust enterprise CA

C. Modify Mobile SSO profiles to use enterprise CA

D. Configure mobile application records in Workspace ONE to trust enterprise CA

E. Modify Workspace ONE authentication policies to use enterprise CA

F. Configure VMware Tunnel network traffic rules to allow access to enterprise CA

Suggested Answer: *ABF*

Juan001 4 years ago

The actual VMware supported answer is

A, C, E

upvoted 1 times

Juan001 4 years ago

The supported answer is

A, C, E

upvoted 1 times

gabrielramos 4 years, 2 months ago

Correct Answer is A, C, E:

https://docs.vmware.com/en/VMware-Workspace-ONE/services/WS1-IDM-deploymentguide/GUID-3EC86F69-6F6E-4C48-A5D9-F319562B6B9C.html

upvoted 2 times

Rabbah_Adel_Ammar 4 years, 4 months ago

A, C and E

upvoted 1 times

Question #29 *Topic 1*

Which component load balances itself through the use of AirWatch Cloud Messaging (AWCM)?

A. VMware Secure Email Gateway

B. VMware Identity Manager Connector

C. VMware AirWatch Cloud Connector

D. VMware Unified Access Gateway

Suggested Answer: *C*
Reference:
https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/1810/WS1-ACC.pdf

Cap9 4 years, 1 month ago
the answer is C

VMware AirWatch Cloud Connector traffic is automatically load-balanced by the AWCM component. It does not require a separate load balancer.
upvoted 1 times

gabrielramos 4 years, 2 months ago
Confirm Correct Answer C:

https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/AirWatch_Cloud_Connector/GUID-AWT-ACC-REQSONPREM.html
upvoted 2 times

nick_name 4 years, 4 months ago
VMware AirWatch Cloud Connector traffic is automatically load-balanced by the AWCM component. It does not require a separate load balancer. Multiple VMware Enterprise Systems Connectors in the same organization group that connect to the same AWCM server for high availability can all expect to receive traffic (a live-live configuration). How traffic is routed is determined by AWCM and depends on the current load.
upvoted 2 times