VMware Identity Manager Smart Card

Authentication

Configuration Guide



Contents

Version History	3
Overview	4
Summary	4
Requirements	4
Browser Support	4
/Mware Identity Manager Configuration	5
Install DoD issued or CA signed certificates	5
Directory Configuration	5
Certificate Authentication Adapter Configuration	6
Access Policy Configuration	8
Identity Provider Configuration	9
Test Login Process	10
Troubleshooting	11
Where are the Logs?	11
My browser is not prompting me for certificates	11
After HA Cluster scale-out of Workspace One Access, Smart Card (CAC) authentication fails.	11
Glossary	14

Version History

Date	Version	Description	Author(s)
11/19/2020	1.0	Initial Draft	Adam Bluhm, Ryan Lakey

Overview

Summary

VMware Identity Manager 3.3.x can be used as an identity and access management solution for vRealize Suite and NSX-T products and doing so brings along the capabilities of vIDM which include certificate based authentication. The focus of this document is the configuration of certificate-based authentication in vIDM for its use with these products. This feature is biased towards Department of Defense Common Access Card (CAC) implementations but may fit other environments as well. This document will not tell you how to implement PKI, only how to integrate vIDM into an existing PKI.

This guide is written for system administrators familiar with the products involved and their terminology.

Requirements

- vIDM 3.3.x as deployed by vRealize Suite Lifecycle Manager 8.x as a single node or cluster.
- OCSP and/or CRL Distribution Points are available for certificate revocation verification.
- If a vIDM cluster is deployed that a load balancer and proper cluster configuration has been done.
- DoD issued certificates are available or an internal authorized CA is available to issue certificates.

This deployment assumes that an enterprise PKI has been deployed. The end user is responsible for having the necessary tokens/cards and middleware so their certificate can be presented to the browser. The certificate selected by the user for authentication must meet the following requirements:

- The certificate will need to have a User Principal Name (UPN) in the Subject Alternative Name (SAN) extension. The UPN needs to correspond to an active directory account.
- The certificate will need to have "Client Authentication" as one of the "Application Policy" or "Enhanced Key Usage" purposes. If the certificate does not have this usage, then it will not be selected by the browser for authentication.

Certificate	Lakey, Ryan Properties
General Details Certification Path Show: <all></all>	Organization Published Certificates Member Of Password Replication Object Security COM+ General Address Account Profile Telephones
Field Value Authority Key Identifier KeyID=0a b0 aa 38 56 47 7b CRL Distribution Points [1]CRL Distribution Point: Distr Certificate Policies [1]Certificate Policy:Policy Ide Subject Key Identifier d3 21 78 07 de 56 08 e3 9b 15 Authority Information Access [1]Authority Info Access: Acc Subject Alternative Name RFC822 Name=Ryan.lakey.ctr Enhanced Key Lisage Smart Card Logon (1 3 6 1 4	User logon name: 11 20550 @mil User logon name (pre-Windows 2000): Comparison (pre-Window
RFC822 Name = Ryan.lakey.ctr Other Name: Principal Name = 11 Fdit Properties	Account options:
Learn more about <u>certificate details</u>	C End of: Saturday . April 16, 2016

FIGURE 1: Example Certificate and Active Directory Account

Browser Support

For certificate-based authentication



- Chrome, Internet Explorer, Microsoft Edge
- Firefox is not supported without additional plugins

VMware Identity Manager Configuration

Install DoD issued or CA signed certificates

- 1. Login to the vIDM appliance configurator by going to https://<appliancefqdn>:8443 and clicking the "Appliance Configurator" link.
- 2. Click on Install SSL Certificates >> Server Certificate tab
- Choose custom certificate and upload the custom certificate here in concatenated PEM format consisting of the issued certificate, subordinate CA cert if any, intermediate CA cert if any, and the root CA certificate. Also supply the private key including the BEGIN and END blocks save.

n ware			
Database Connection	>	Soprer Certific	to Beecknuck Cetificate. Trucked CAs
Install SSL Certificates	· ·		
Mobile SSO	>		Install a public certificate and private key on the primary Identity Manager server port (443).
Identity Manager FODN	-		In most cases SSL is terminated at the load balancer. Make sure to upload the appropriate certificate on the load
Configure Syslog	· ·		balancer.
Change Password	-	SSL Certificate	Custom Certificate
Sustam Socurity			O Auto Generate Certificate (self-signed)
es Eile Lesstiere	-	SSL Certificate Chain	BEGIN CERTIFICATE MIIDujCCAqKgAwIBAgIGAXW+n5jRMA0GCSqGSIb3DQEBCwUAMFMxMzAxBgNV
og File Locations	2		BAMM KnZSZWFsaXplIFN1aXRlIExp2mVjeWNsZSBNYW5h22VyIExvY2tlciBDQTEP
ime Synchronization	>		MAUG AluEcgwGVk13YXJlMQswCQYDVQQGEwJJTjAeFw0yMDExMTIyMjQyMTFaFw0y Misy
			njex MTIVNJQVMTFAMEYXGTAXBGNVBAMMECouZW5nLnZtd2FyZS5jb20xDTALBgNV za m
			BENBU BENBUKEXDTALBGNVBAOMBENNQlUXCZAJBGNVBAYTAlVTMIIBIjANBGKqhkiG
			9W05 AQEFAAOCAQ8AMIIBCgKCAQEA3Ci8ewo95dr6Aaj/N/J1Y4JxJpOUeD47aJqi 👻
			Example Format
		Private Key	Private key not shown
			Example Format
		Subject Alternative Names	cava-6-246-014.eng.vmware.com
			Please provide SAN (optional), separated by a comma. SAN on be a Evily Qualified Domain Name (EDDNI) or can be a wildeard domain name (i.e. * domain com or * store domain com) instead of a
			multiple-level wildcard (i.e *.* domain.com)
		Appliance Self Signed Root CA Certificates	https://cava-6-246-014.eng.vmware.com.443/horizon_workspace_rootca.pem You might need this URL when configuring the load balancer.
			Save

Figure 2: Server Certificate Installation

- 4. (Optional) Repeat the steps on the Passthrough Certificate tab but this may be unnecessary in some configurations such as a single node or a cluster that is not terminating SSL on the load balancer.
- 5. Repeat for any additional nodes for a cluster deployment.

Directory Configuration

- Login to the vIDM appliance configurator by going to https://<appliancefqdn>:8443 and clicking the "Identity Manager Admin Console" link or it can be accessed by logging into https://<appliancefqdn> as a user with administrative rights and then choosing "Administrative Console" from the drop down under your username.
- 2. Navigate to the Identity & Access Management tab and choose Directories.
- 3. Click on the directory name for your Active Directory directory.



4. Ensure UserPrincipalName is selected for the Directory Search Attribute.

<back directories<="" th="" to=""><th></th><th>Settings</th><th>Identity Providers Sync Log</th></back>		Settings	Identity Providers Sync Log	
°18	Directory Name*	AD for Sync Connection - IWA		
Yt:		 Active Directory over LI Active Directory (Integr 	DAP ated Windows Authentication)	
AD for Sync Connection - IWA Domain(s):	Directory Sync and Authentication	Select the connector that syn	ics users from Active Directory to the VMware Identity Manager directory.	
		Sync Connector	· · ·	
		Identity Providers	WorkspaceIDP1	
Type: Active Directory with IWA		Directory Search Attribute*	UserPrincipalName 👻	
connector.			Enter the account attribute that contains the user name.	
Sync now	Certificates	If your Active Directory requir certificate. If there is more that each certificate is in the PEM	es STARTTLS encryption, select the check box below and provide the Root CA an one Root CA certificate, add all the certificates one after another. Make sure format with the delimiter lines "BEGIN CERTIFICATE" and "END CERTIFICATE".	
Delete Directory		This Directory requires	all connections to use STARTTLS	
	Join Domain Details	Enter the name of the Active	Directory domain to join and the domain admin user name and password.	
		Domain Name*		
		Domain Admin Username*	-	
	Allow Change Password	Allow Active Directory Users	to change password.	
		Enable Change Passw	ord	
	Bind User Details	Enter the user name and pas required domains. For the us is different from the Join Dom domain is the fully-qualified d	sword of the bind user, who has permission to query users and groups for the er name, enter the sAMAccountName, for example, jdoe. If the bind user's domain vain entered above, enter the user name as sAMAccountName@domain, where lomain name. For example, jdoe@example.com.	
		Bind User Name*		
		Bind User Password*		
			Enter your Active Directory bind account password.	
		Save Cancel		

Figure 3: Directory Configuration

Certificate Authentication Adapter Configuration

- Login to the vIDM appliance configurator by going to https://<appliancefqdn>:8443 and clicking the "Identity Manager Admin Console" link or it can be accessed by logging into https://<appliancefqdn> as a user with administrative rights and then choosing "Administrative Console" from the drop down under your username.
- 2. Navigate to the Identity & Access Management tab and click the setup button on the top right and choose Connectors.
- 3. Click on the worker link for the target connector.
- 4. Select the Auth Adapters tab then click on the CertificateAuthAdapter link.
- 5. Click the checkbox to enable the Certificate Adapter.
- 6. Upload the subordinate, intermediate, and root CA certificates for the issued Smartcard certificates used in the environment or optionally just upload all DoD CA certs.

uthentication Adapter	
Name *	CertificateAuthAdapter
Enable Certificate Adapter	
Root and intermediate CA certificates *	
	Select File
	You can upload multiple DER and PEM root and intermediate CA certificates including concatenated PEM files
Uploaded CA Certificates	CH-DOD EMJ, CJ-JJ, CU-PRI, CU-DD, CU-JS, Growmmert, C-US (SP12451025717C11827127C11820821980739712720520852984471738C1) X CH-DOD EJJ, CU-PRI, CU-DD, CU-JS, Growmmert, C-US (SP12451026282205098471738512885598447173861) X CH-DOD EJJ, CU-PRI, CU-DD, CU-JS, Growmmert, C-US (SP1245102628220509847172861) X CH-DOD EJJ, CU-PRI, CU-DD, CU-JS, Growmmert, C-US (SP12451026282205098471728712782588578444712471) X CH-DOD EJJ, CU-PRI, CU-DD, CU-JS, Growmmert, C-US (SP12451026282205098471728712782588578444712471) X CH-DOD EJJ, CU-PRI, CU-DD, CU-JS, Growmmert, C-US (SP124510260810271444712471) X CH-DOD EJJ, CU-PRI, CU-DD, CU-JS, Growmmert, C-US (SP1251025780257085204471247) X CH-DOD EJJ, CU-PRI, CU-DD, CU-JS, Growmmert, C-US (SP135102574625780257085204471247) X CH-DOD EJJ, CU-PRI, CU-DD, CU-JS, Growmmert, C-US (SP1351035044471247110711E57126258857144447124711071125722885714447124071125712581 X CH-DOD EJJ, CU-PRI, CU-DD, CU-JS, Growmmert, C-US (SP13510350444712471727278245520508510467178789777267124572 X CH-DOD EJJ, CU-PRI, CU-DD, CU-JS, Growmmert, C-US (SP1351035044471247172782454447124655885144471097105112611288572703 X CH-DOD EJJ, CU-PRI, CU-DD, CU-JS, Growmmert, C-US (SP1351035044712471277248244471246558851444710971051112611288572703 X CH-DOD EJJ, CU-PRI, CU-DD, CU-JS, Growmmert, C-US (SP1351035024944427147211261091094717117117043044713447117011156112011261144447144710111561126112611444471447101115611261144447144710111561126114447144714471144711447144714471447144

Figure 4: Certificate Auth Adapter Configuration 1

- 7. (Optional) Enable certificate revocation while not required for this to work will be required by STIG and is a good idea anyway. OCSP is preferred over CRL also and if your OCSP responder has a certificate it must be uploaded here too.
- 8. Enable the Consent Form option and input the standard DoD login banner in the Consent Form Content box.
- 9. Save and repeat for any other connector appliances in a clustered deployment.

Unor Identifier Search Order		
User luentitier search Order	Laph	
Validate UPN Format		
	Validate the format of the UserPrincipalName field	
Request Timeout	0	
	Trimeout in seconds to wait for a response. A value of zero will wait indefinitely.	
Certificate Policies Accepted		Delete
	Add another value	
	Object Identifier (OID) list that is accepted in the Certificate Policies extension	
Enable Cert Revocation		
	Check box to enable revocation checks	
Use CRL from Certificates		
	Check box to use the CRL Distribution Points extension of the certificate	
CRL Location		
	CRL location to use for revocation check (e.g. http://crlutl.crl or file./i/crlFile.crl)	
Enable OCSP Revocation		
Use CRL in case of OCSP failure		
	Check box to use CRL if OCSP fails	
Send OCSP Nonce		
	Check box to include a nonce in OCSP request	
OCSP URL		
	OCSP URL to use for revocation check (e.g. http://ocspurl.com).	
OC SP URL Source	Configuration Only	
	Source for OCSP URL: configuration, certificate or both	
OCSP Responder's Signing Certificates	Select File	
	You can unload multiple DER and PEM anonder's partiticates	
Unloaded OC SP Signing Cortificator		
Eachle Concent Form before Authentication		
Enable Consent Form before Authentication	Center box to include a consent form window before looging in using certificate authentication	
Consent Form Content	Non-second second	
consent rom content	tou are accessing a c.s. dovernment (God) information system (IS) that = Is provided for USG-authoritied use only.	
	By using this IS (which includes any device attached to this IS), you consent to the following conditions:	
	-The USG routinely intercepts and monitors communications on this IS	
	The proper antendamp on the statest or protocol statest contract of the protocol statest of the protoc	
	-At any time, the USG may inspect and seize data stored on this IS.	
	-Communications using, on data stored on, this IS are not subject to routine monitoring, interception, and search, (

Figure 5: Certificate Auth Adapter Configuration 2. Note revocation configuration not shown.



Access Policy Configuration

- Login to the vIDM appliance configurator by going to https://<appliancefqdn>:8443 and clicking the "Identity Manager Admin Console" link or it can be accessed by logging into https://<appliancefqdn> as a user with administrative rights and then choosing "Administrative Console" from the drop down under your username.
- 2. Navigate to the Identity & Access Management tab then select Policies
- 3. Edit the default access policy or create a new one
- 4. Under configuration click on the 3 dots for the network range for Web Browsers
- 5. For "then the user may authenticate using" select Certificate
- 6. Configure fallback methods as needed for local directory or password authentication if certificate authentication fails or is unable to be performed due to OCSP unavailability or other environmental issues.
- 7. Save and exit.

Edit Policy					×
1 Definition 2 Configuration	You can create a list of ru of devices that can acces application before reauth	les to access the applications se s the applications, the auth meth enticating.	lected. For each rule, sel lods, and the maximum r	ect the IP network range number of hours users ca	, the type in use the
3 Summary	Network Range	Device Type	Authentication	Re-authenticate	
	: ALL RANGES	Web Browser	Password+1	8 Hour(s)	×
	: ALL RANGES	Workspace ONE App	Password+1	2160 Hour(s)	×
	ADD POLICY RULE				

Figure 6: Access Policy Configuration 1

vmware[®]

< CONFIGURATION	Edit Policy Rule	
If a user's network range is "	ALL RANGES v	0
and user accessing content from *	Web Browser ~	•
and user belongs to group(s)	Q Select Groups	•
	Rule applies to all users if no group(s) selected.	
Then perform this action	Authenticate using v	0
then the user may authenticate using *	Certificate v	• •
If the preceding method fails or is not applicable, then	Password (Local Directory) ~	• •
If the preceding method fails or is not applicable, then	Password v	●
	ADD FALLBACK METHOD ■	
Re-authenticate after *	8 Hours v	- 1
Advanced Properties 🛩		
	Custom Error Message 🌑	
	Custom Error Message	
	CANCE	SAVE

Figure 7: Access Policy Configuration 2

Identity Provider Configuration

- Login to the vIDM appliance configurator by going to https://<appliancefqdn>:8443 and clicking the "Identity Manager Admin Console" link or it can be accessed by logging into https://<appliancefqdn> as a user with administrative rights and then choosing "Administrative Console" from the drop down under your username.
- 2. Navigate to the Identity & Access Management tab then select Identity Providers
- 3. Select the default "WorkspaceIDP_1" IDP or if a different one has been created and in use select that one.
- 4. Verify Certificate is shown under Authentication Methods and the connectors you configured earlier are listed.
- 5. Under IdP Hostname verify the appliance name is shown in a single node deployment or the cluster name in a clustered deployment.

Identity Providers (3)						Add Identity Provider
Identity Provider Name	Auth Methods	Directory	Network Ranges	Connector(s)	Туре	Status
System Identity Provider	Password (Local Directory)	System Directory	ALL RANGES		Built-in	Enabled
Built-in					Built-in	Enabled
WorkspaceIDP_1	Certificate Password	AD for Sync Connection - IWA	ALL RANGES		Identity Manager	Enabled





Figure 9: Identity Provider Configuration 2

Test Login Process

You should now be able to login to vIDM and be shown the DoD login banner and be prompted for certificates from your Smart card.

vmware[®]

Troubleshooting

Where are the Logs?

/opt/vmware/horizon/workspace/logs/connector.log

/opt/vmware/horizon/workspace/logs/horizon.log

My browser is not prompting me for certificates

Verify your browser trusts the Root CA and chain for the vIDM certificate. If the browser does not trust the vIDM URL you are browsing to it will not present your certificates for selection.

After HA Cluster scale-out of Workspace One Access, Smart Card (CAC) authentication fails.

vmware[®]

Error

Incorrect issuer in SAML AuthnRequest.

This is a bug with how vRealize Lifecycle Manager 8.x scales out an HA Cluster for Workspace One Access. Luckily there is a fairly simple way to permanently resolve the issue. This only impacts you if your customer has a pre-existing Workspace One Access/vIDM Linux appliance and you then go scale-out to an HA cluster using vRealize Lifecycle Manager.

The issue is that vRealize Lifecycle Manage in the scale-out process deploys the secondary appliances via an OVA but then attempts to copy all the pertinent settings from the primary node to the secondaries. While it does a good of this there is one area that has yet to be fixed in the code. And that is when users attempt to authenticate to the HA Cluster via any load balancer (with or without SSL Termination (both work)), users get a SAML error and the logs reveal little else.

- The Lifecycle Manager scale-out to turn vIDM into an HA cluster is somehow different than the way it's done without Lifecycle Manager.
- Lifecycle Manager did copy over all the certificates from the primary to the OVF deployed secondary nodes but something went wrong
- It turns out that the secondaries were unable to see the certs it said it had from UI and the config-state.json file thus causing auth issues
- It was only when clearing out the certs in the config-state.json file and then re-uploading the certificates that authentication worked.

The related Bugzilla details can be found here (VPN required):

- https://bugzilla.eng.vmware.com/show_bug.cgi?id=2638633
- https://bugzilla.eng.vmware.com/show_bug.cgi?id=2633131

The fix action is to do the following:

- 1. ssh to both the secondary appliances as root
- 2. stop horizon service:
 - a. service horizon-workspace stop
- 3. cd /usr/local/horizon/conf/
- 4. copy the current config-state.json file before editing:
 - a. cp config-state.json config-state.json.bak
- 5. Use 'vi' or 'vim' to edit the config-state.json file
- a. vim config-state.json
- 6. Now you need to search for the keyStore keyword with the following command:
 - a. /keyStore
- 7. You are looking for "keyStoreFile" and "keystore" with all the certificates.



i.

For "keyStoreFiles" you should see something similar to this: a.

- "idpAdapterConfig" : { 545
- 546 "com.vmware.horizon.adapters.certificateAdapter.CertificateAuthAdapter" : {
- "enableOCSP" : null, 547 "validateUpn" : "false" 548
- "keyStore Files" : "[\"CN=DOD EMAIL CA-34, OU=PKI, OU=DoD, O=U.S. Government, C=US 549
- (F089A39D657A2F38527E7C111E36DBEDB30021F889740F96FCF8F5839F3729CB)\",\"CN=DOD ID CA-40, OU=PKI, OU=DoD, 0=U.S. Government, C=US (9D125EA16DCA38447B2456D3E02531418067399771237C52882C59B44767884C)\",\"CN=DOD ID CA-41, OU=PKI, OU=DoD, O=U.S. Government, C=US (081BA940884B4FB343458A09F04B2EC0A36CDA339ECA95C55BED5A96034A6852)\",\"CN=DOD ID CA-52, OU=PKI, OU=DoD, 0=U.S. Government, C=US (30AE2DB2585A2E8225DC969A7062B64EB948E3ADFC069792ACA1C493180992A5)\",\"CN=DOD EMAIL CA-51, OU=PKI, OU=DoD, O=U.S. Government, C=US

(AE8820DB38D5F304A94A8724471D311E0F6D205889378AAA7270A916F5BAFCA4)\",\"CN=DOD EMAIL CA-33, OU=PKI, OU=DoD, O=U.S. Government, C=US (F38198D97A7DA6CF1F876091C6D8CAB4F0E549439649A51B7F4FB7A0E58BC0C7)\",\"CN=DOD ID CA-33, OU=PKI, OU=DoD, O=U.S. Government, C=US (B1670A585295DA03BC84AAF080F96DF2F0E425C26D056A396E5EFBB4485FF8B7)\",\"CN=DOD ID CA-42, OU=PKI, OU=DoD, 0=U.S. Government, C=US (378C3F90E2F6D885C0D39F439716F4780B2C95EE5409F6044FE21C011947CE20)\",\"CN=DOD SW CA-57, OU=PKI, OU=DoD, O=U.S. Government, C=US (00931153E93114CD00AEF166913AA9CD45B6E3AA07389005426D3FE78BBB9720)\",\"CN=DOD EMAIL CA-52, OU=PKI, OU=DoD, O=U.S. Government, C=US

(86175108108A290A1922A79272F9EDA4A4663A03A099DB683196166179973367)\",\"CN=DOD ID SW CA-47, OU=PKI, OU=DoD, O=U.S. Government, C=US (62F03DBA240625294340231EB45E1DB91B0994F70F14FD81C1A9882AB4E38E50)\",\"CN=DDD SW CA-55, OU=PKI, OU=DDD, O=U.S. Government, C=US (5EE0842B2D7B2F11B4CD8B4EC6BE2EF2B5100271514B583F8D3223561C70711E)\",\"CN=DOD ID SW CA-48, OU=PKI, OU=DoD, O=U.S. Government, C=US

(7A3E25A1F120DECD208FCACB3C5BBE3261344CE82358C94F68A135E5739B35AE)\",\"EMAILADDRESS=unknown@vmware.com, CN=Internal Root CA myrootca 23462, OU=Horizon-Workspace, O=VMware, L=Palo Alto, ST=california, C=US

b. But you must delete all the certificate entries so that is looks like this (below is the exact command and syntax): "keyStoreFiles" : "[]", i.

For "keystore" you should see something like this: c.

- "enableCertRevocation" : "" 559
 - "certificatePolicies" : null,
 - 560 561 "consentForm" : "\"You are accessing a U.S. Government (USG) Information System (IS) that is provided for USGauthorized use only.\n\nBy using this IS (which includes any device attached to this IS), you consent to the following conditions:\n\n-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.\n\n-At any time, the USG may inspect and seize data stored on this IS.\n\n-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.\n\n-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.\n\n-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details. \""

562 "keystore"

"AAMsMILT2zCC0x4wgZQGCSqGSIb3DQEFDTCBhjBkBgkqhkiG9w0BBQvwVvRAzGR+NF2NXqMH+mLqi9I1LuuU7GVeBPELXrpfn0LtdDI34+vY7gd7y3zF7W0 zx65j/WBhRP0dWv4hWVWwbcmZpQICBAACASAwDAYIKoZIhvcNAgsFADAeBg1ghkgBZQMEAS8wEQQMrviT4Dw0t0wnQguoAgEIBILSg4MN/sUx+M1NKBWTxwK dziQxyYg9tGJ08a69hI0g8R6tRJUdTpw+HWnLc3GumqIgNZRHLbB4FDcWgojHXsNDDP33L+9BzCkUqiESkeK1pH/YDyXsVhGUA58HY8U1C/2Rqezr4mvdkjL TkVURfjcYLo1zwE49rTHVB3itPEzI8sbwl7JV2wPB02PWtidC0yKPZ027mUQZCARrMskCBmHmYecUJoihQptdmEASrj6JD1cE6HIchwzIkJnlt7j7xKM31oh 6iTAXSB7Et6YJIabkLruQZODo8XtbmuHkR0d2skfUtcB2IXmluhuIxMV07dwCLmEBKeSGYPPHEBD00yV76vzlpnVQqUvC6K3MpS/4Qq/pFVQFanegYu0+nBR E2FVZgNvj0ksvMGSwnvNYm3HdyMz7E6W+hISwXrR70+zzx9lDxZdST014CuNu9ZI57bqhnKbeMVm7u5Jc9iCSU/7lfzzcizsD5nw5N8BsMz6iYRcuGjsOXIK BPcSC4d1eFEuwzC0rQzcpzgrMMoOfwQ/6QcyBMojFiGeSbOON8illzjjmSwONlBmVzfFfr/2/gATibsaD8704mbK/cCn54lV/ZeBrTir11YNZ0FYgwadAMeD LbO+47VpzOAjwHqnGoZ4zBtlZhuudPJ/z678mwDsRUX6+eAgBED0I5BbPPtKIQdTryP6eSpVPargEJI7K3lV6TgPRE089VQ61rvKbgQBC7J8Cq/Ex4iRSqez jZK9NhwvxpHV7/wJrgjgtJHfqheJPX7lWIq4Eql05+6ujV6q6aVJj5jnbgqj/oLZQ0mjN9YU7ToupP/2036SSbziuj5oZDKUbwZ5HOr/aqEGzUfcQVA4lYDW Icb5gTZppQeF5vVjllWGRHDCWXb6XMJ0l/ErZyAzcBrWBrM7EQCuZ9hDtkzRasssop50+VfSgEHr2oyPNZsliYII2A7d9iTRIoQIcI+AGkoQeaKpAU0i0DuF hUHa+g0g2Tma0Q4heoYAu&rBEyjH/0rrfX3Eyg4bhpz01+auBk/5KpwrCCWcoofBgXzxLlBBLkb3i/LSbJFiL2dt2ZUKXjyg0xJPeKV0StXLAWAb/lprVLV/ jFs+UewCJHTlB3obUM0UQ3/qt3R8VBRyKzxiog8+Y/g/+WBvc1xYTGYRG8zyDCkk7+xgKlJgvpijzUJ014sKnxEvxni42CncnDcGsj9KKoULCVzDT46FI0AN jlFA1HgjKVJD/SDudiRUWxqKfkjUcGwAbSZN+hIAFPITXEY04YyPB4IMk08HlT1Nu4vriQ4gcdFBKDk1Bg1zQsb5BU4eIBijVbrRPTQbI6XajkIZ9YhQl1VC

But you must delete all entries so that it looks like this (below is the exact command and syntax): d.

- i. "keystore" : null,
- Now save and close the file with the following commands: 8.
 - e. Press the ESC button

i.

- f. :wa!
- 9. start horizon service: service horizon-workspace start
- 10. Wait about 3 minutes
- 11. Login to the individual node (appliance) you just edited via the web UI
- 12. Click on "Identity & Access Management" > "Setup" > "Connectors" > Click on the 'Worker" for the secondary node you just edited.
- 13. Next Click "Auth Adapters" > "CertificateAuthAdapter"
- 14. Click on 'Select File' to re-upload all your DoD Root and Intermediate certificates. Also, if you are doing SSL termination then it would not hurt to upload your load balancer certificates as well.
 - Example: g.





- 15. Now you can test CAC authentication and it should work.
- 16. DONE!

NOTE: If you can't authenticate or things don't look right then re-check your json file for typos. This method works.

Glossary

Smart Card/CAC	The CAC, a "smart" card about the size of a credit card, is the standard identification for active duty uniformed Service personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel. It is also the principal card used to enable physical access to buildings and controlled spaces, and it provides access to DoD computer network and systems.
User Principal Name	In Windows Active Directory, a User Principal Name (UPN) is the name of a system user in an email address format. A UPN (for example: john.doe@domain.com) consists of the user name (logon name), separator (the @ symbol), and domain name (UPN suffix).
PEM	Privacy-Enhanced Mail (PEM) is a de facto file format for storing and sending cryptographic keys, certificates, and other data, based on a set of 1993 IETF standards defining "privacy-enhanced mail."





VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 vmware.com Copyright © 2020 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at vmware.com/go/patents. VMware is a registered trademark or trademark of VMware, Inc. and its subsidiaries in the United States and other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies. Item No: vmw-wp-tech-temp-a4-word-101-proof 6/20