Avoiding an Identity Crisis

AUTHENTICATION WITH WINDOWS SERVER CONTAINERS

Steven Follis

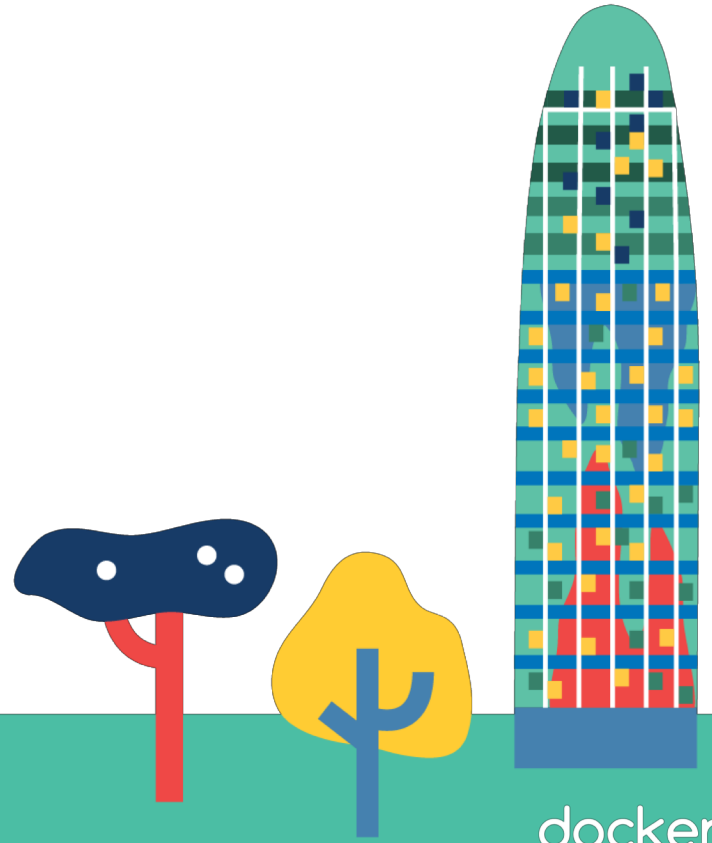
Solutions Engineer

Docker Inc.

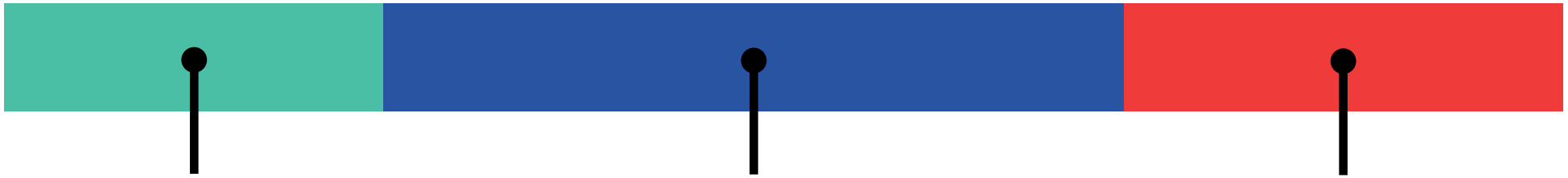
Israel Vega

Principal PM Manager
Commercial Software Engineering (CSE)

Microsoft



Today



Authentication Options

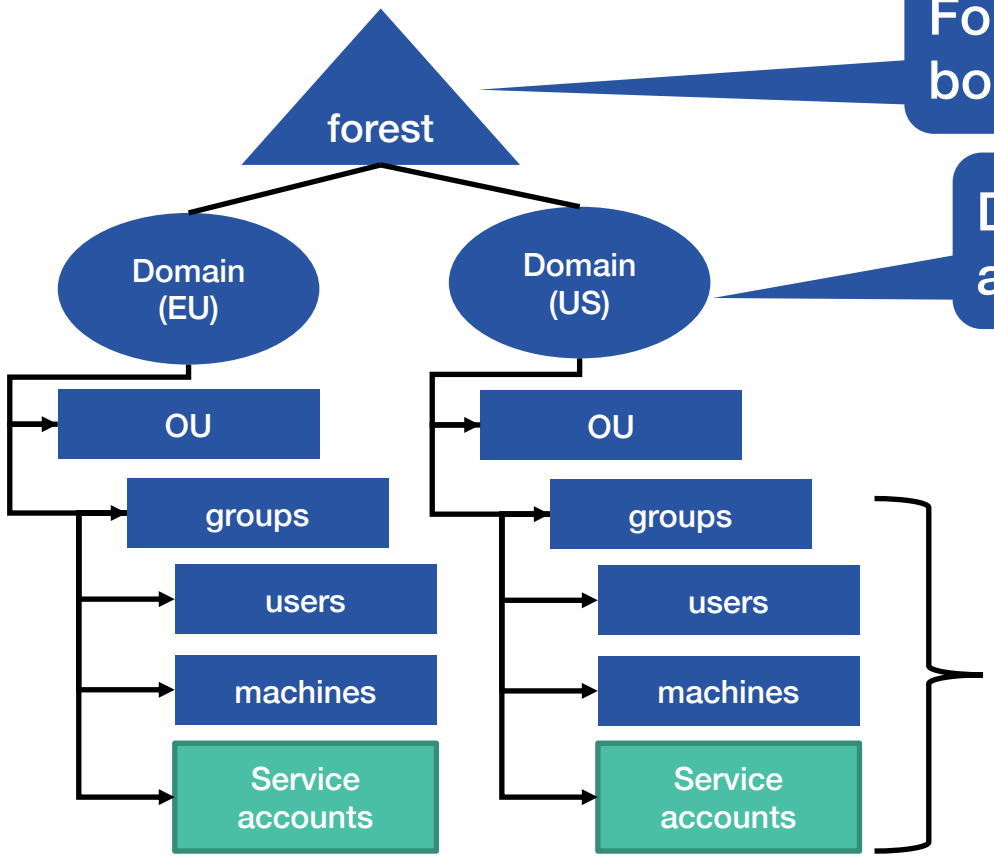
Container Authentication

Clustered Environments


Active Directory
dockercon18
EUROPE

AD Basics – Logical Concepts

FQDN: corp.winid.net

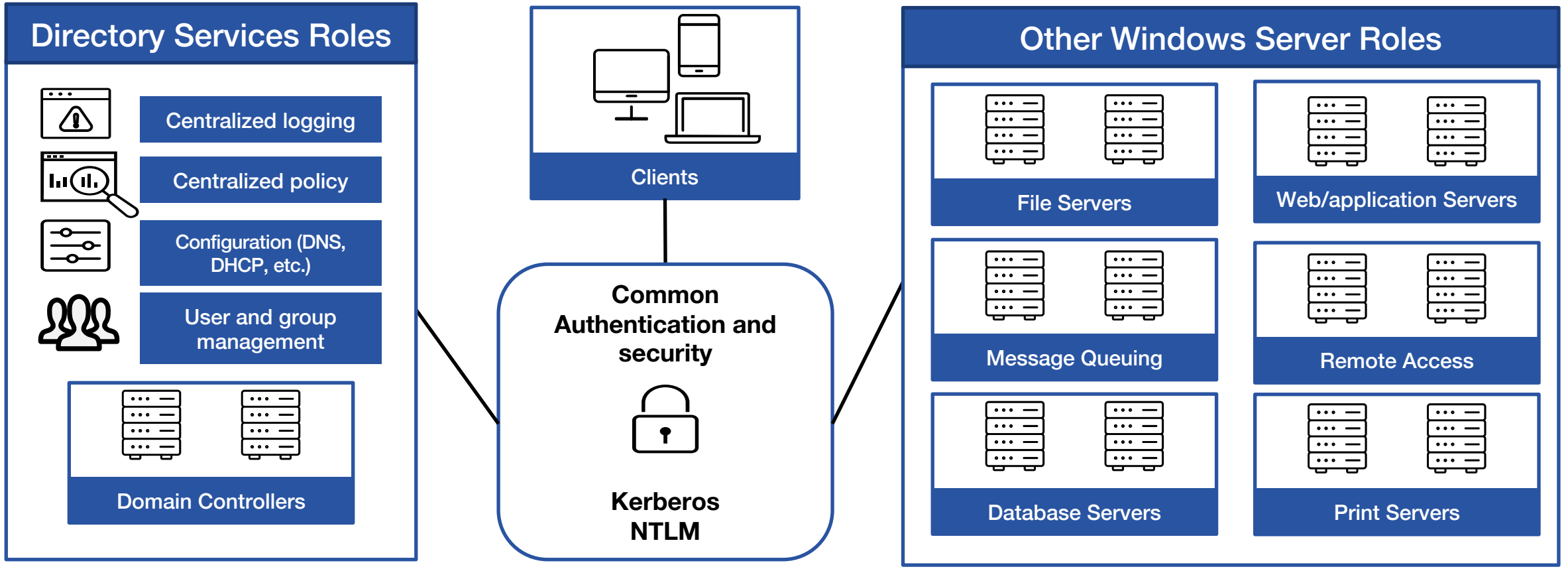


Forest=Top most security boundary

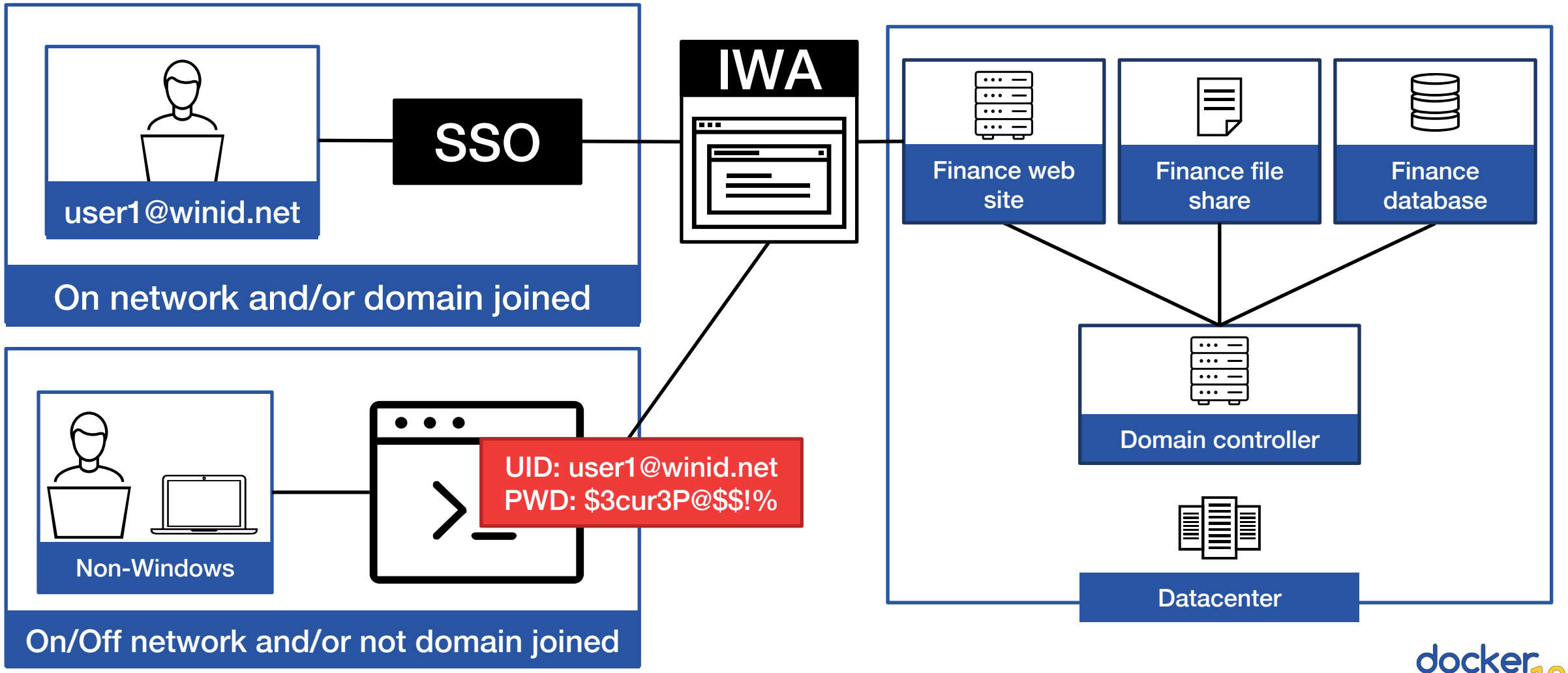
Domains=Replication and security boundary

Schema Objects= Identified by schema type, SIDs, sAMAccount Names, FQDNs, etc.

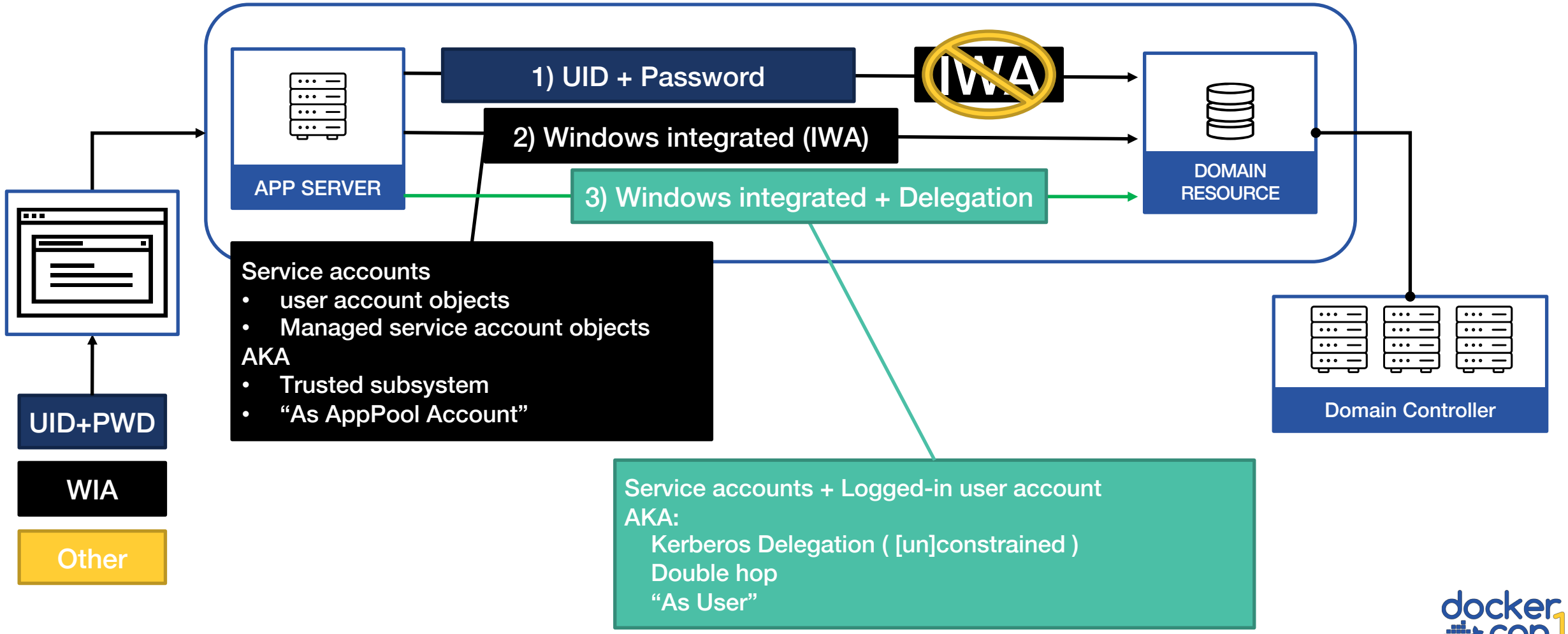
AD Basics – Physical Concepts



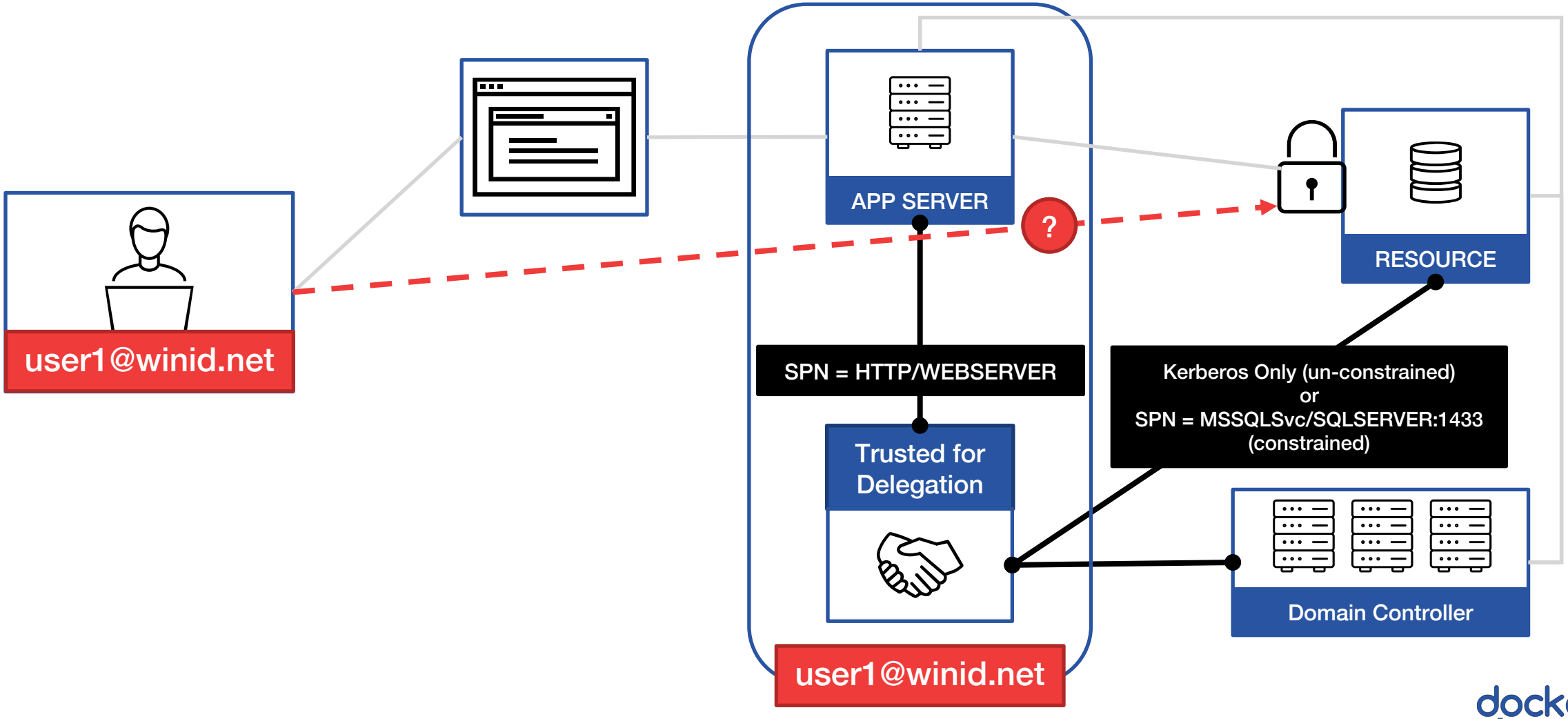
Integrated Windows Authentication (clients)



Integrated Windows Authentication (machines/apps)

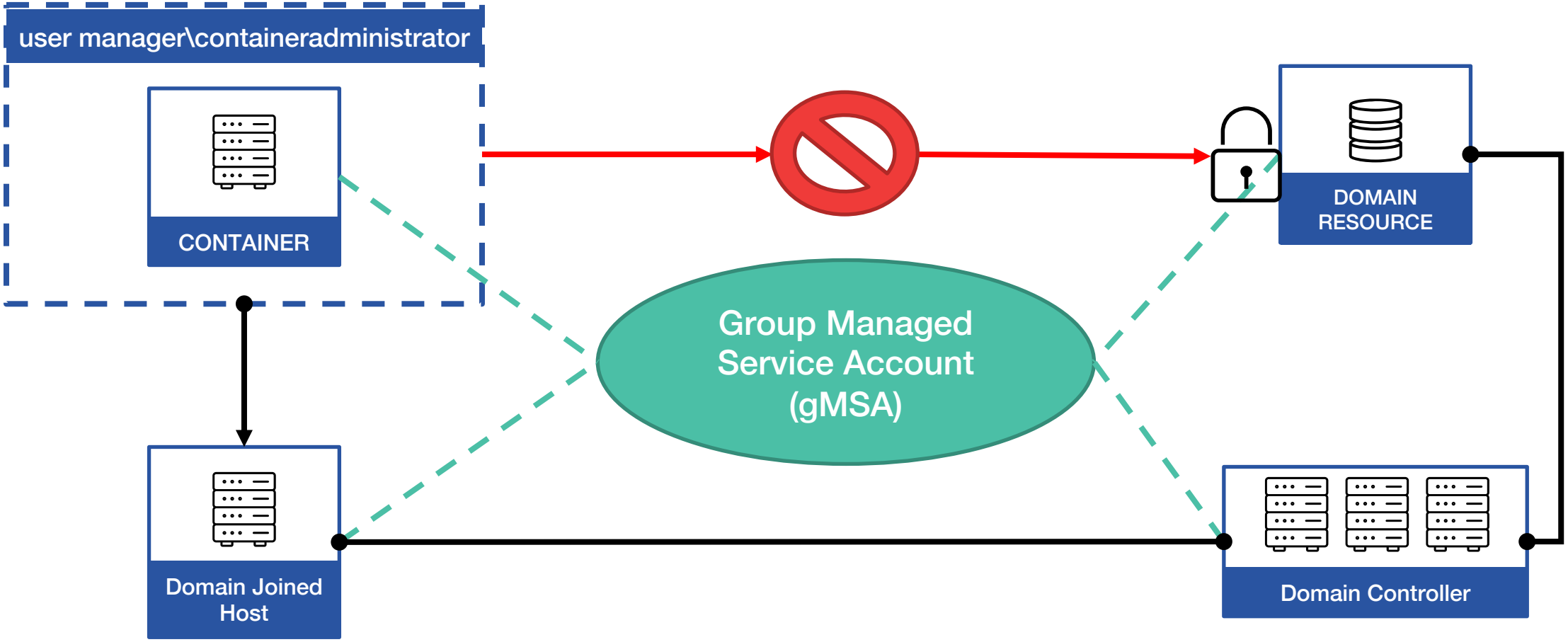


Kerberos [Un]Constrained Delegation

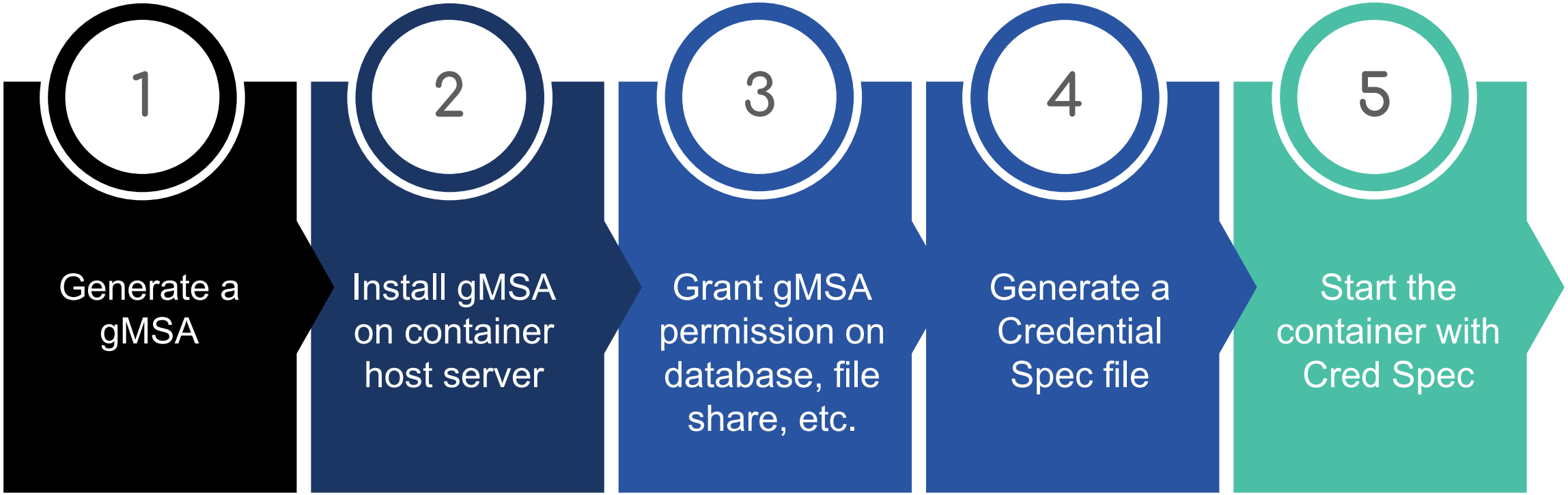


Windows Container Authentication

Windows Containers and IWA



Setting up a gMSA



Walkthrough: Setting Up a gMSA

Set Up Key Distribution & Hosts

```powershell
#Run this as a Domain Admin

#Run this once in the forest - CAUTION-Do not force replication in large environments
Import-Module ActiveDirectory
Add-KdsRootKey -EffectiveTime ((get-date).addhours(-10));

#Create a group to hold the container hosts
$containerHostName = "YOUR CONTAINER-HOST MACHINE NAME"
$containerHostGroupName = "YOUR GROUP NAME FOR HOSTS i.e ContainerHosts"
$containerHostGroupDisplayName = "DISPLAY NAME FOR YOUR GROUP i.e Windows Container Hosts"
New-ADGroup -GroupCategory Security -Name $containerHostGroupName -DisplayName
$containerHostGroupDisplayName -GroupScope Universal

#Add the container host machines to the group
Add-ADGroupMember -Members (Get-ADComputer -Identity $containerHostName) -Identity $containerHostGroupName

#Validate that they were created-You will need to reboot the servers to update the membership
Get-ADGroup -Identity $containerHostGroupName
```

Create a key to generate passwords

Create a group of computers that can access the gMSA password

Set Up the gMSA Account

```
#For each gMSA
$gmsaAccount = "YOUR GMSA SAMACCOUNT NAME"
$gmsaAccountFQDN = "YOUR GMSA FQDN"
$containerHostGroupLdapCN = "YOUR CONTAINER HOSTs GROUP LDAP PATH i.e `
                    CN=ContainerHosts,CN=Users,DC=corp,DC=winid,DC=net"
```

Create a new gMSA

```
New-ADServiceAccount -Name $gmsaAccount -DNSHostName $gmsaAccountFQDN `
-PrincipalsAllowedToRetrieveManagedPassword  "Domain Controllers", "Domain Admins", $containerHostGroupLdapCN `
-KerberosEncryptionType RC4, AES128, AES256 `
-ServicePrincipalNames HTTP/$gmsaAccount, HTTP/$gmsaAccountFQDN
```

Additional configuration may be needed for delegation

Install GMSA & Generate Cred Spec

```
#On the Container Host
Install-ADServiceAccount -Identity $gmsaAccount
Test-ADServiceAccount -Identity $gmsaAccount
```

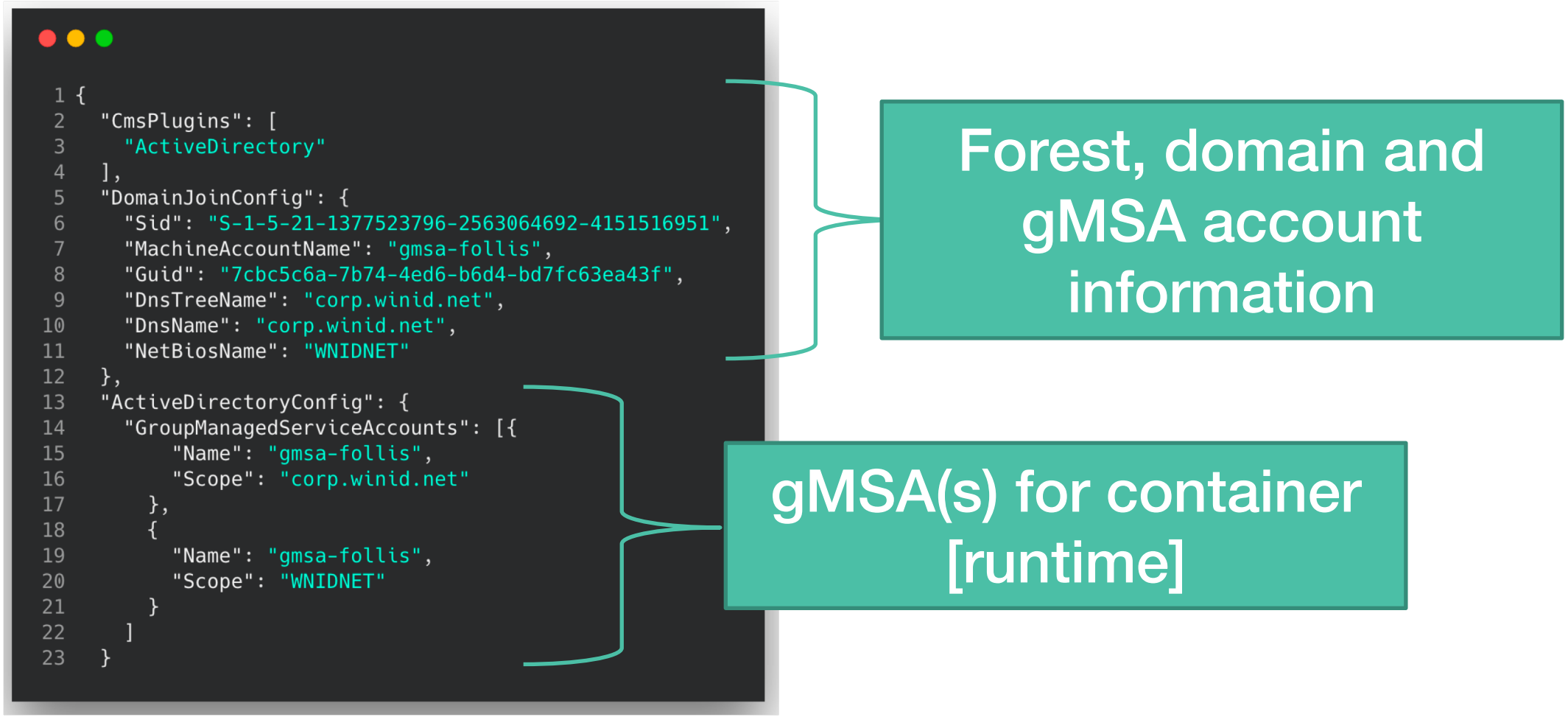
Install the gMSA on the container host

```
 Invoke-WebRequest
"https://raw.githubusercontent.com/Microsoft/Virtualization-
Documentation/live/windows-server-container-
tools/ServiceAccounts/CredentialSpec.psm1" -UseBasicParsing -OutFile
$env:TEMP\cred.psm1

Import-Module $env:temp\cred.psm1
New-CredentialSpec -Name "$gmsaAccount-gmsa" -AccountName $gmsaAccount `
    -Domain $(Get-ADDomain -Current LocalComputer)
Get-CredentialSpec
```

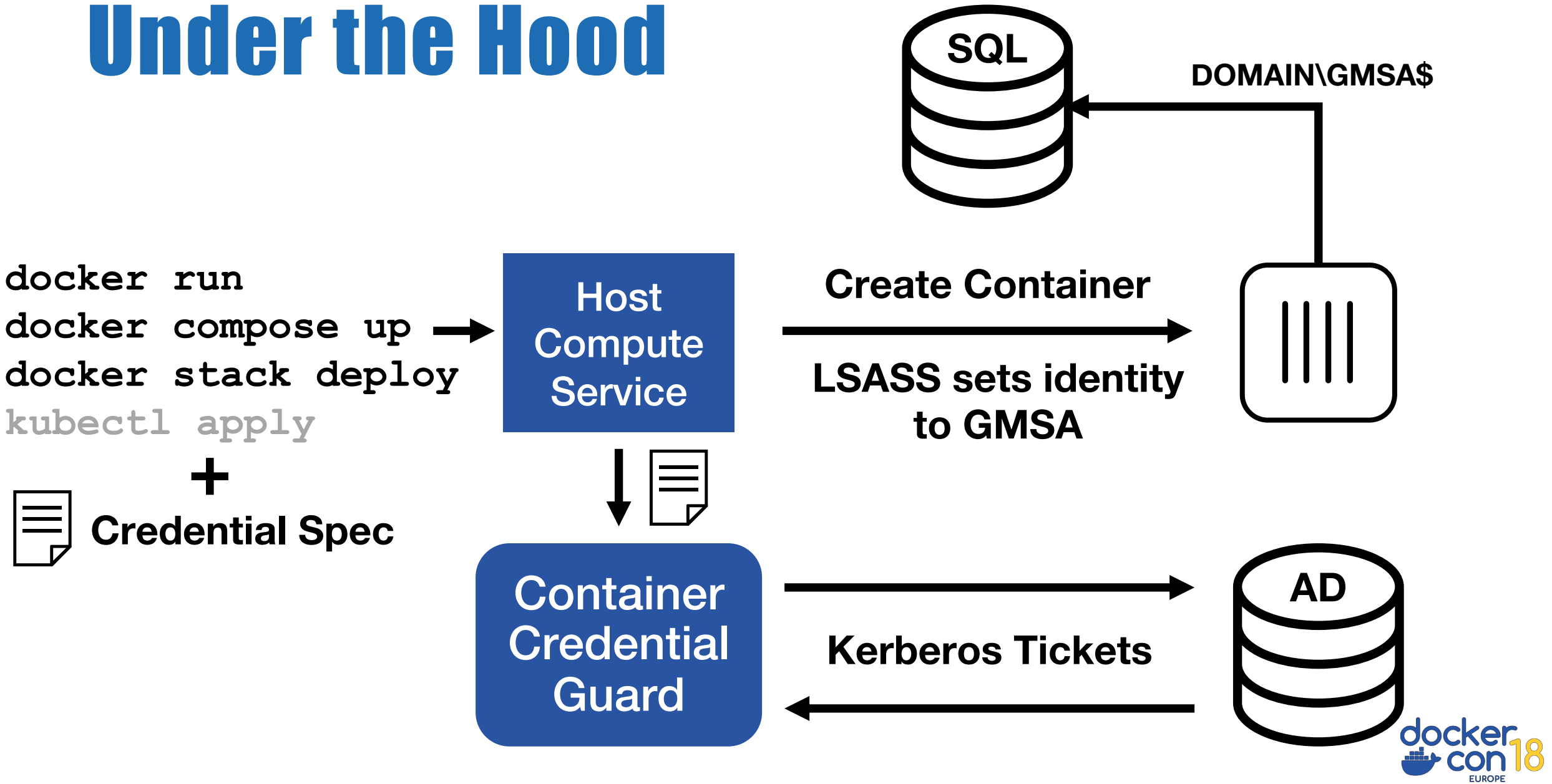
Create a new Credential Spec based on the gMSA

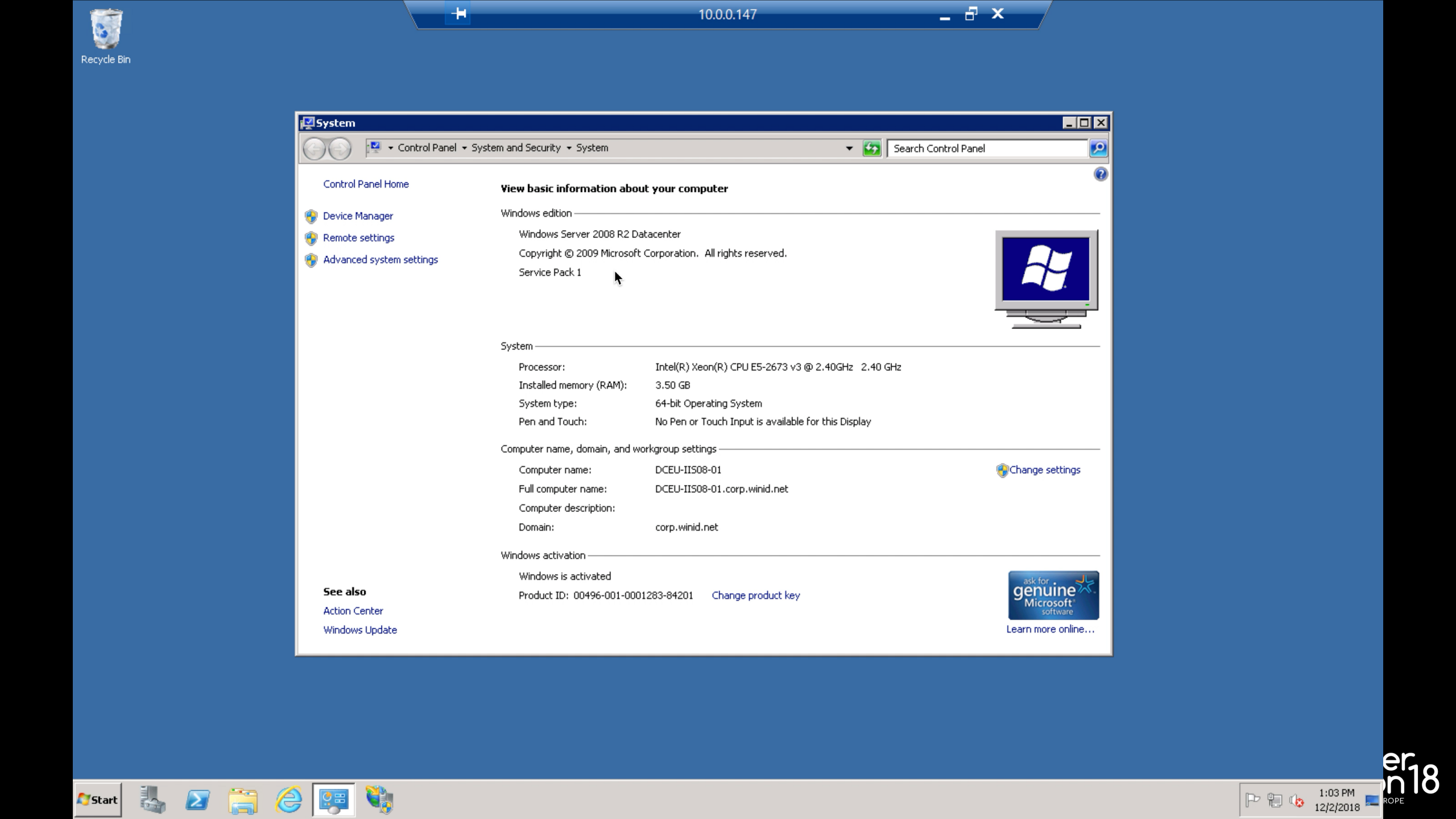
Credential Spec File




```
New-CredentialSpec -Name gmsa-follis -AccountName gmsa-follis -Domain $(Get-ADDomain -Current LocalComputer)
```

Under the Hood




10.0.0.147
Recycle Bin
System
Control Panel ▸ System and Security ▸ System
Search Control Panel
Control Panel Home
Device Manager
Remote settings
Advanced system settings
View basic information about your computer
Windows edition
Windows Server 2008 R2 Datacenter
Copyright © 2009 Microsoft Corporation. All rights reserved.
Service Pack 1
System
Processor: Intel(R) Xeon(R) CPU E5-2673 v3 @ 2.40GHz 2.40 GHz
Installed memory (RAM): 3.50 GB
System type: 64-bit Operating System
Pen and Touch: No Pen or Touch Input is available for this Display
Computer name, domain, and workgroup settings
Computer name: DCEU-IIS08-01
Change settings
Full computer name: DCEU-IIS08-01.corp.winid.net
Computer description:
Domain: corp.winid.net
Windows activation
Windows is activated
Product ID: 00496-001-0001283-84201
Change product key
ask for genuine Microsoft software
Learn more online...
See also
Action Center
Windows Update
Start
1:03 PM
12/2/2018

IWA + Kerberos with Containers Quick Reference

Front End Login	Access to Backend Resource	Will Succeed	Requires gMSA	Notes
Anonymous, Basic, Other non-Windows	Trusted Subsystem with UID and PWD	Yes	No	Use UID and PWDs to connect to back end resources
Anonymous, Basic, Other non-Windows	IWA “As User”	No *	No *	No Windows User account to logon with
IWA	Trusted Subsystem	Yes	Yes	Configure GMSA to access back end resources or use UID and PWDs
IWA	IWA “As User”	Yes	Yes	Requires Kerberos delegation

*** Will work with identity/protocol transition or manual impersonation**

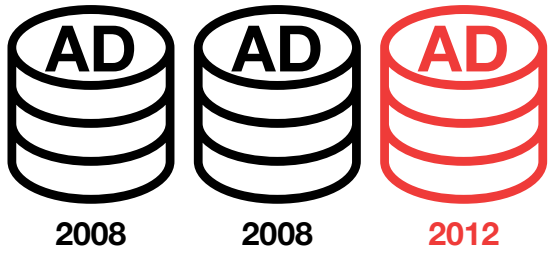
Demo: Authentication Scenarios in Windows Containers

Cluster Operations

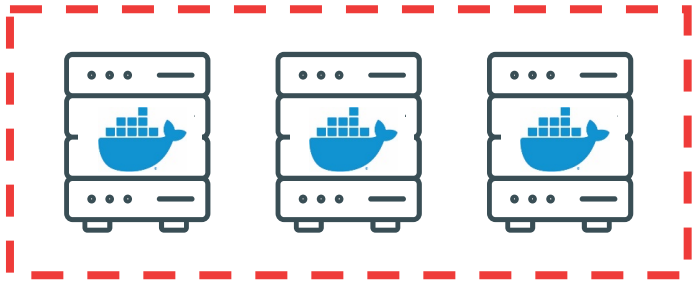
docker con 18
EUROPE

Working with your AD team

1. Deploy a 2012 DC



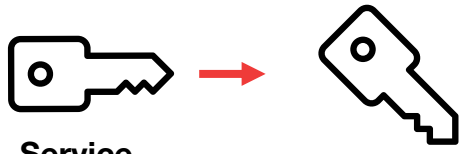
2. Group the nodes



3. Distribute Cred Specs

4. Business Process

5. Map permissions



Kubernetes

Coming Soon

Support for Windows Server worker nodes expected to move from Beta to GA in Kubernetes v1.14

Initial Windows support will ship ***without*** the ability to use gMSAs

Alpha expected in 2019

Gotchas

- Windows Server 2016 Caveats (addressed in Windows Server 2019)
  - The AD Service Principal Name (SPN) used when creating the gMSA must match the container hostname specified at creation time

```
docker run -d --hostname $gmsaAccount -p 80 `
   --security-opt "credentialspec=file://web1.json” `
   dtr.moby.io/finance/webapp:103
```

  - GMSAs must be unique (1:1 GMSA:Container)
  - Instability when running gMSA containers with Hyper-V isolation

Resources

Presentation GitHub
https://github.com/stevenfollis/dceu18-windows-identity

Microsoft Docs: Active Directory Service Accounts for Windows Containers
https://docs.microsoft.com/en-us/virtualization/windowscontainers/manage-containers/manage-serviceaccounts

Deployment Walkthrough
https://github.com/MicrosoftDocs/Virtualization-Documentation/tree/live/windows-server-container-tools/ServiceAccounts

GitHub: Credential Spec Creation PowerShell Module
https://github.com/MicrosoftDocs/Virtualization-Documentation/blob/live/windows-server-container-tools/ServiceAccounts/CredentialSpec.psm1

Migrate Legacy Windows Before End of Support

For more information visit:

https://dockr.ly/WindowsServerUpgrade

Gracias!

Common Questions with Windows Containers

Can I use Azure AD, AWS IAM or other IDP?

- Not directly. You can use it to authenticate to your app using OAuth/Claims for the front end, but you can't use it for back end services (accept some cloud services).

Can I use Azure Active Directory Domain Services (ADDS)?

- No since you need to be able to manage the GMSA which requires domain admin permissions

Can I use an Azure Managed Service Identity?

- No. The identity type is an Azure AD Service Principal, not a valid Windows credential

Can I use a certificate?

- It depends, some applications support cert based auth, but you may still need a valid Windows identity

What about ADFS/PING/SiteMinder or other federation IDPs?

- May be used to authenticate users for front-ends, but back-end services may still need a GMSA

Identifying Patterns in Existing Applications

- Try and login and view the auth flow
  - Are you prompted for credentials? If so, which credentials?
  - Do you need access to all resources or just the application?
- For web apps, check the web.config
  - IdentityImpersonate=true, AuthenticationMode=Integrated
  - Connection strings with embedded user ids, or trusted connection
- Get an account for the application and/or ask how someone gets access
  - Do they need to add you to a group?
  - Does the group have access to the app and the backend?
- For SQL Databases, as the DBA for access
- Look for impersonation code, file system writes, database connections, LDAP calls, MSMQ