Identity Management for Cloud and Hybrid Cloud Environments

Red Hat Enterprise Linux 7 and Azure Active Directory Domain Services

Mahesh Unnikrishnan
Principal Program Manager
Microsoft Identity Division

Mark Heslin
Principal Technical Program Manager
Red Hat Infrastructure Business Unit
Goals

1. Introduce Azure Active Directory Domain Services (AD DS)

2. Show how/where/why Azure AD DS can be used

3. Understand how on-premise applications running on Red Hat Enterprise Linux 7 system can be moved to Azure
Agenda

- Overview
- AD Options
- Components
- Cloud Configuration
- Hybrid Configuration
- Q&A
- Futures
- Summary
Azure Active Directory

- Secures Azure, Office 365 & all Microsoft services
- SSO to 1000s of apps, 1 identity
- Connect & sync identities from on-premises directories
- Multi-factor authentication
- Device registration
- Rich integration with 2500+ SaaS apps
- Conditional access control
- Self-service password reset
- Standards based platform (OAuth, OIDC, SAML, WS-Fed, REST) for modern app development.
- Privileged identity management
- B2C directories
- B2B collaboration
- Azure AD Domain Services
Azure Active Directory – by the numbers

- **9.5M** Azure AD Directories
- **600 M** users + 4 B consumers
- **Identify 30K** potentially compromised users per day
- **Identity ML system processes 10TB** of data/day
- **>1.3 B** Enterprise Auths/Day + 13 B Consumer Auths/Day
- **>35K** active 3rd party apps
- **automatically deflect 1.5M** attacks per day (consumer)
- **23,000** customers with EMS/Azure AD Premium
Why do we need another Active Directory option???
Satisfying identity needs of applications migrated to the cloud.

1. VPN Gateway/ExpressRoute connection
2. Domain Controller VM in Azure
Azure AD Domain Services - Overview

• A fully managed service from Microsoft
  • No need to provision, patch, backup, monitor domain controllers in the cloud

• Powered by Azure AD. Integrates with your on-premises directory
  • Use the same corporate credentials to access Office 365, apps migrated to Azure or on-premises applications

• ‘Lift-and-shift’ applications to Azure with ease
  • Available for your cloud applications without the need for a VPN/ExpressRoute connection
  • Use LDAP, NTLM, Kerberos, Domain-join, Group Policy etc.

• Easily spin up a managed AD domain for dev/test environments

• Easy to set-up, pay as you go
Azure AD Domain Services - Features (1)

1. Simple 2-click deployment – ready for use in about 20 minutes.
2. Single managed domain (*with custom domain name*) per Azure AD directory.
3. Highly available (HA) domain
4. Domain join – Windows/Linux
5. Powered by Azure AD – Use your corporate credentials
   *same users, group memberships, passwords*
6. Windows integrated authentication (Kerberos, NTLM)
7. LDAP bind and LDAP read support
Azure AD Domain Services - Features (2)

8. Secure LDAP (LDAPS) support – including over internet
9. Create custom Organizational Units (OU)
10. Administer DNS
11. Basic Group Policy: single built-in GPO each for users & computers container
12. Use familiar management tools *(AD Admin Center, AD PowerShell)*
13. Service available in multiple Azure Regions:
   - Europe: West-Europe, North-Europe
   - Asia: East-Asia, Southeast-Asia
   - Australia: East-Australia, Southeast-Australia
How do I know which Active Directory option to choose?
Active Directory Options - On-Premise

- All systems are deployed *on-premises*
- AD – Windows Server Active Directory
- Red Hat Enterprise Linux hosts *directly integrate* to Active Directory via `sssd`
- Red Hat Enterprise Linux 7 preferred – simplifies, streamlines integration via `realmd`
Active Directory Options – In Cloud (Azure VM)

- Similar to on-premise deployment, except all systems are located *in-cloud* (Azure VM)
- AD - Windows Server VM deployed in Azure Infrastructure Services
- Red Hat Enterprise Linux VMs *directly integrate* to Active Directory via *sssd*
- Red Hat Enterprise Linux 7 preferred – simplifies, streamlines integration via *realm*
Active Directory Options – Azure AD Domain Services

- RHEL systems are deployed *in-cloud* (Azure VM)
- AD – managed service provided by Azure Active Directory Domain Services
- Red Hat Enterprise Linux VM(s) *directly integrate* to Azure AD DS via sssd
- Red Hat Enterprise Linux 7 preferred – simplifies, streamlines integration via realmd
Active Directory Options – Hybrid with “Lift and Shift”

1. On-premise AD identities - sync’d to Azure AD using Azure AD Connect
2. New Red Hat Azure VM deployed and joined to AD DS Domain
3. On-premise application re-deployed to Red Hat Azure VM
4. Authentication uses original on-premises credentials
# Active Directory Based Offerings – Feature Comparison

<table>
<thead>
<tr>
<th>Feature</th>
<th>Windows Server Active Directory (on-premises install)</th>
<th>Windows Server Active Directory (cloud install – Azure VMs)</th>
<th>Azure Active Directory Domain Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cloud-based?</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Pay-as-you-go?</td>
<td>N</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Ease of deployment</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Easy</td>
</tr>
<tr>
<td>Managed Service?</td>
<td>N</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Highly Available?</td>
<td>Y (Implementation dependent)</td>
<td>Y (Implementation dependent)</td>
<td>Y</td>
</tr>
<tr>
<td>LDAP Bind, Read Support?</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>LDAP Write Support?</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
</tr>
</tbody>
</table>
What components does it need to work???
Azure AD Connect

Simple tools to bridge your identity infrastructure across on-premises Active Directory and the cloud.

Azure AD Connect synchronizes users and groups to Azure AD.

Password hashes can be optionally synchronized; authentication is completed against Azure Active Directory.

Federation can be optionally configured using ADFS; authentication is passed back through federation and completed against Windows Server Active Directory.
SSSD (System Security Services Daemon)

- Preferred client for Red Hat Enterprise Linux
- Access to different identity, authentication providers (e.g. - Active Directory, IdM, LDAP native, LDAP w/Kerberos)
- Extensible (new identity, authentication sources)
- Supports off-line caching of user credentials (clients)
- Reduces load on identity servers
- Provides file sharing capabilities (RHEL 7.2)

*Extensible, enhanced alternative to Winbind*
realmd (realm discover)

• Package that manages discovery and enrollment of Linux clients to AD or IDM domains
• Domain clients/providers supported:
  – SSSD = IdM and AD
  – Winbind = AD
• By default, realmd sets up SSSD’s AD provider
• Advanced features available – one-time password for join, custom OUs, etc.
• Easy to use:
  
  # realm discover                      ! Discover all domains (requires NetworkManager)
  
  # realm discover ad.example.com       ! Discover a particular domain
  
  # realm join ad.example.com           ! Join a domain
How does it work in “the cloud”?
Azure AD Domain Services for cloud environments

e.g. dev/test environments, cloud-only organizations
Cloud Configuration (1)

Step 1. Configure Azure AD Domain Services *(Cloud)*

- Create the delegated administration group (‘AAD DC Administrators’) 
- Create or Select Azure Virtual Network 
- Enable Azure AD Domain Services 
- Update DNS Settings for Azure Virtual Network 
- Enable Password Sync 

Cloud Configuration (2)

Step 2. Provision Red Hat Enterprise Linux Client *(Cloud)*

- Select from Azure Marketplace *(or import image through Red Hat Cloud Access program)*
- Specify hostname, local username, password, VM size, etc.
- Join the VM to the same Azure virtual network as Azure AD Domain Services
  *...Wait for deployment to complete and VM to start up...*
- Configure sudoers file
- Register system
- Update system

Cloud Configuration (3)

Step 3. Join Red Hat Enterprise Linux Client to Azure AD DS domain *(Cloud)*

- SSH to the VM
  
  # ssh -l local-user rhel7-vm

- Install required packages

  # sudo yum install realm sssd krb5-workstation krb5-libs

- Kerberos initialize

  # kinit bob@CONTOSO.COM

- Discover and join to the domain

  # sudo realm discover CONTOSO.COM

  # sudo realm join CONTOSO.COM -U 'bob@CONTOSO.COM'

Cloud Configuration (4)

Step 4. Verify domain join *(Cloud)*

- SSH to the VM using the domain account
  
  # ssh -l bob@CONTOSO.COM rhel7-vm.cloudapp.net

- Verify the user home directory was initialized
  
  # pwd

- Confirm the user and group ID match Azure AD Domain Services
  
  # id

Cloud Configuration (5)

Step 5. Deploy/configure application *(Cloud)*

- Deploy application
- Test application
Ok - what about the “Hybrid” configuration?
Azure AD Domain Services for hybrid environments
Integrate with your corporate on-premises AD
Hybrid Configuration - Prerequisites

1. On-premise AD infrastructure
   - Previously configured and fully functional:

2. On-premise Red Hat Enterprise Linux client
   - Previously configured and fully functional

3. Domain Administrator privileges
   - Required to setup Azure AD Connect

4. On-premise application
   - Fully configured and ready to move to Azure
Hybrid Configuration (1)

Step 1. Provision AD Sync Server *(On-premise)*
- Provision Windows Server 2012 R2 system/VM
- Download latest version of Azure AD Connect
- Install using Express settings
- Configure sync features – password sync, attribute filtering, writeback, etc.

Hybrid Configuration (2)

Step 2. Configure Azure AD Domain Services *(Cloud)*
- Create the delegated administration group (‘AAD DC Administrators’)
- Create or Select Azure Virtual Network
- Enable Azure AD Domain Services
- Update DNS Settings for Azure Virtual Network
- Enable Password Sync

Hybrid Configuration (3)

Step 3. Provision Red Hat Enterprise Linux Client *(Cloud)*

- Select from Azure Marketplace *(or import image through Red Hat Cloud Access program)*
- Specify hostname, local username, password, VM size, etc.
- Join the VM to the same Azure virtual network as Azure AD Domain Services
  
  ...*Wait for deployment to complete and VM to start up*...

- Configure sudoers file
- Register system
- Update system

Hybrid Configuration (4)

Step 4. Join Red Hat Enterprise Linux Client to Azure AD DS domain *(Cloud)*

- SSH to the VM
  
  ```
  # ssh -l local-user rhel7-vm
  ```

- Install required packages
  
  ```
  # sudo yum install realm sssd krb5-workstation krb5-libs
  ```

- Kerberos initialize
  
  ```
  # kinit bob@CONTOSO.COM
  ```

- Discover and join to the domain
  
  ```
  # sudo realm discover CONTOSO.COM
  
  # sudo realm join CONTOSO.COM -U 'bob@CONTOSO.COM'
  ```

Hybrid Configuration (5)

Step 5. Verify domain join *(Cloud)*

- SSH to the VM using the domain account
  
  ```
  # ssh -l bob@CONTOSO.COM rhel7-vm.cloudapp.net
  ```

- Verify the user home directory was initialized
  
  ```
  # pwd
  ```

- Confirm the user and group ID match Azure AD Domain Services
  
  ```
  # id
  ```

Hybrid Configuration (6)

Step 6. Deploy/configure application (Cloud)

- Deploy application
- Test application
Active Directory Options – Hybrid with “Lift and Shift”
Demo
Questions?
Futures

- Azure Active Directory Domain Services
  - Currently in Public Preview
  - GA planned for Fall 2016*

* Feedback welcome on better-together scenarios with Red Hat Enterprise Linux or feature requests
Summary (1)

Azure AD Domain Services

- Available today (*tech preview*)
- “Lift-and-shift” applications to Azure more easily
- Use LDAP, Active Directory domain join, NTLM and Kerberos authentication
- Provides a managed, highly-available service
- Get started quickly, pay as you go
- Develop, test with no identity worries
- Manage Azure virtual machines effectively using Group Policy
Summary (2)

Red Hat Enterprise Linux 7 systems

- Integrate quickly, easily via *realmd*
- Provide the ideal platform for *on-premise, cloud and hybrid* cloud applications
Secure your seat for these security sessions

- **Secure your enterprise software supply chain with containers**
  Tuesday, 10:15 AM - 11:15 AM, Room 2005

- **Red Hat security roadmap**
  Tuesday, 11:30 AM - 12:30 PM, Room 2005

- **Are you listening to what SELinux is telling you?**
  Tuesday, 3:30 PM - 4:30 PM, Room 2005

- **Identity management for cloud and hybrid cloud environments with Red Hat and Microsoft**
  Tuesday, 4:45 PM - 5:45 PM, Room 2005

- **Security Enhanced Linux for Mere Mortals**
  Tuesday, 4:45 PM - 5:45 PM, Room 2006

- **Cryptography: What every application developer needs to know**
  Tuesday, 4:45 PM - 5:45 PM, DevNation Room 132

- **Practical steps implementing Red Hat identity management solution**
  Wednesday, 10:15 AM - 11:15 AM, Room 2005

- **End-to-end OpenSCAP for automated compliance**
  Wednesday, 11:30 AM - 12:30 PM, Room 2005

- **Middleware security: Authentication, authorization, and auditing services**
  Wednesday, 3:30 PM - 4:30 PM, Room 2005

- **Container security reality check: The container is only the beginning**
  Wednesday, 4:45 PM - 5:45 PM, Room 2006

- **Running a policy-based cloud with Cisco Application Centric Infrastructure, Red Hat OpenStack, and Project Contiv**
  Wednesday, 4:45 PM - 5:45 PM, Room 2005

- **Red Hat identity and access management vision, solution, and roadmap**
  Thursday, 10:15 AM - 11:15 AM, Room 2005

- **Understanding security risks and mitigation across the virtualization stack**
  Thursday, 11:30 AM - 12:30 PM, Room 2005

- **Compliance, security automation, and remediation with CloudForms, Satellite, and Ansible**
  Thursday, 3:30 PM - 4:30 PM, Room 2005
For more information

- References
- Getting Started with Azure AD Domain Services
- Visit us in the Partner pavillion
  - Red Hat + Microsoft Pod (In Red Hat Booth)
  - Microsoft Booth
Thank you - don't forget to complete your survey!!!
References
References (1/3)

Red Hat Enterprise Linux
Red Hat Enterprise Linux 7 Installation Guide

SSSD (System Security Services Daemon)
SSSD – AD Integration
• https://fedorahosted.org/sssd/wiki/Configuring_sssd_with_ad_server

realmd
realmd – AD Integration
References (2/3)

**Microsoft Windows Server 2012 R2**

Install and Deploy Windows Server


Deploy Active Directory


**Azure AD DS**


**Azure AD Connect**

Microsoft Azure

- https://azure.microsoft.com/en-us/overview/what-is-azure/

Cloud Configuration Steps

Azure Active Directory Domain Services – Get Started

How to Join a Red Hat Enterprise Linux 7 VM to a managed domain

Red Hat Cloud Access

- https://access.redhat.com/articles/1989673  (Running Red Hat Enterprise Linux in Azure)
LEARN. NETWORK. EXPERIENCE OPEN SOURCE.