DELL EMC

Technical Note

JOINING VXRAIL SUPPLIED VCSA AND PSC TO ACTIVE DIRECTORY

Abstract

This guide describes the procedures for joining the VxRail Supplied vCenter Server Appliance (vCSA) and Platform Services Controller (PSC) to an Active Directory Domain as well as the procedures for attaching the users and groups from this Active Directory domain to the vCenter Single Sign-On domain. The procedures are presented for both vSphere 6.5 and vSphere 6.7 environments.

October 2018

TABLE OF CONTENTS

Introduction

This paper describes the procedure for joining the VxRail Supplied vCenter Server Appliance (vCSA) and Platform Services Controller (PSC) to an Active Directory domain. Furthermore, it describes the procedure for attaching the users and groups from this Active Directory domain to the vCenter Single Sign-On domain. These operations are highly critical and require not only very strong skills in vSphere/vCenter administration but also a good understanding of services such as Active Directory Domain Services, Domain Name System and Network Time Protocol.

Specifically, this paper presents these procedures in a prescriptive step-by-step manner. Due to the prescriptive nature of the procedures and to make it easier to perform the procedures, they are presented in separate sections for vSphere 6.5 and vSphere 6.7 despite the fact the differences between the two versions are minor and involve only some navigation and screen changes.

Intended Audience

This document is intended for Customers and Dell EMC Service providers who are authorized to work on a VxRail Cluster and VxRail Administrators.

Overview of the Relevant Concepts

There are certain requirements involving name resolution as well as time synchronization of the system components for the proper configuration and correct functioning of Active Directory authentication. These requirements are addressed by services like DNS and NTP. Figure 1 illustrates how these services come together to provide the solution in a VxRail cluster environment at high level. In this section we provide a brief overview of these services and the relevant concepts associated with these services.

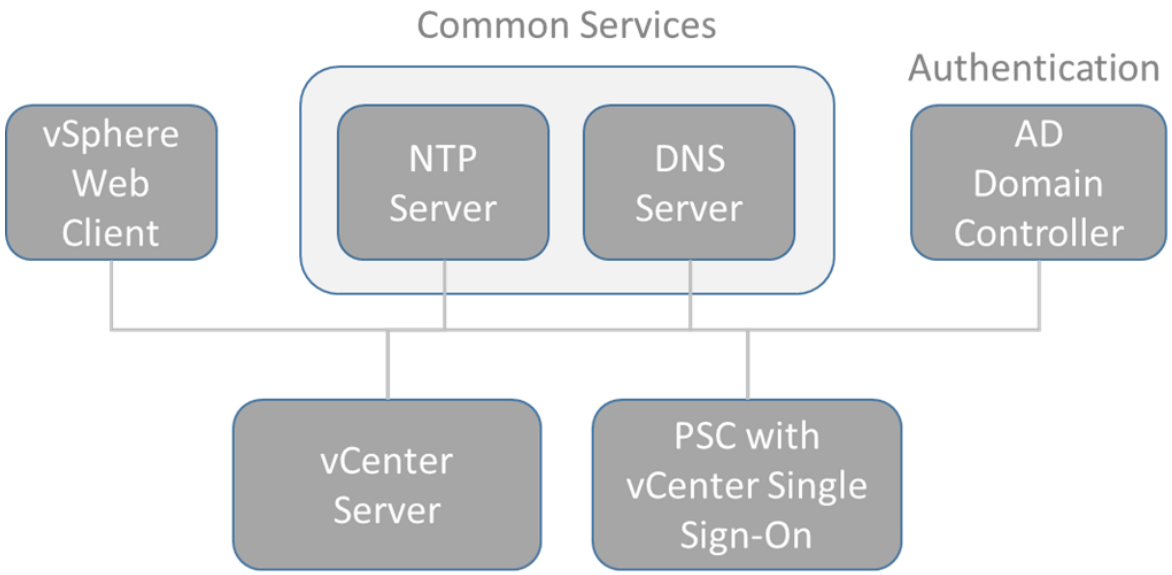

Figure 1 **Solution Architecture at High Level**

Active Directory Domain Services

Active Directory Domain Services (AD DS or simply AD), is the cornerstone of every Windows domain network. It stores information about members of the domain, including devices and users, verifies their credentials and defines their access rights. The server(s) running this service is called a domain controller. A domain controller is contacted when a user logs into a device, accesses another device across the network, or runs a line-of-business into a device. Many other Active Directory services as well as most of Microsoft server technologies rely on or use Domain Services. Organizations can use AD DS in Windows Server to simplify user and resource management while creating scalable, secure, and manageable infrastructures.

There are a couple of pitfalls regarding Active Directory configuration, which must be avoided:

- If you employ a Windows-based Active Directory service, do not use the machine that has the same Security Identifier (SID). Refer to this resource for details.
- Do not copy/clone an existing Windows Server for new AD installation

For an overview of AD DS, you can refer to the "Active Directory Domain Services Overview".

For installation of AD, you can refer to the "Install Active Directory Domain Services".

Domain Name System

Domain Name System (DNS) is not a component of Active Directory, however, it has a direct impact on the Active Directory logical structure design. AD uses DNS name resolution services to make it possible for clients to locate domain controllers and for the domain controllers that host the directory service to communicate with each other. Therefore it is essential to understand the core features of DNS such as delegation, recursive name resolution, and Active Directory-integrated DNS zones (see "Creating a DNS Infrastructure Design" for more details).

There is a DNS requirement for vCSA and PSC as well. The requirement is that both forward and reserve zones are configured properly. When a vCSA is deployed, the installation of the Web server component that supports the vSphere Web Client fails if the installer cannot look up the appliance FQDN from its IP address. The reverse lookup is implemented using PTR records. Please see "DNS Requirements for the vCenter Server Appliance and Platform Services Controller Appliance" for more details.

Time Synchronization

vSphere components are very sensitive to time synchronization. Therefore, all components on the vSphere network must have their clocks synchronized (see "Synchronizing Clocks on the vSphere Networks"). If the clocks on the machines in a vSphere network are not synchronized, SSL certificates, which are time-sensitive, might not be recognized as valid in communications between network machines. Unsynchronized clocks can result in authentication problems, which can cause the installation to fail or prevent the vCenter Server Appliance vpxd service from starting.

When you turn on periodic time synchronization, VMware Tools sets the time of the guest operating system to be the same as the time of the host. However, native time synchronization software, such as Network Time Protocol (NTP) for Linux and the Mac OS X, or Microsoft Windows Time Service (Win32Time) for Windows, is typically more accurate than VMware Tools periodic time synchronization and is therefore preferred. NTP is used to synchronize computer clocks in a network so that an accurate clock value, or time stamp, can be assigned to network validation and resource access requests. The Windows Time service can be run in NTP mode. The service integrates NTP and time providers, making it a reliable and scalable time service for enterprise administrators.

Time synchronization is especially critical for the proper operation of many Windows services and applications. Therefore, any Windows host machine on which vCenter Server runs must be synchronized with the Network Time Server (NTP) server (see this Knowledge Base article). The Windows Time service synchronizes the date and time for all computers running in an AD DS domain. The Windows Time service is essential to the successful operation of Kerberos authentication and, therefore, to AD based authentication. Any Kerberos-aware application, including most security services, relies on time synchronization between the computers that are participating in the authentication request. AD domain controllers must also have synchronized clocks to help to ensure accurate data replication.

In order to update the NTP server in Windows for time synchronization, type the following commands at the command prompt:

```
w32tm /config /manualpeerlist:"NTP_Server_IP_Address" /syncfromflags:manual
/reliable:yes /update

net stop w32time

net start w32time
```

To synchronize ESXi clocks with an NTP server, you can use the VMware Host Client (see "vSphere Single Host Management" for this task).

Joining VxRail PSC to AD

The VxRail follows the external deployment model for vCSA and PSC. That is, the vCSA and PSC reside on their own virtual machines. Once a VxRail cluster is initialized, a VxRail embedded vCenter Server Appliance and a Platform Services Controller are deployed and running on the VxRail cluster. The vCSA links with the PSC. In order to configure permissions so that users and groups from the AD can access the vCenter Server components, PSC instance must first join to the AD domain. To enable an Active Directory user to log in to the vCenter Server instance that uses an external PSC, as is the case for the VxRail Supplied vCSA and PSC, by using the vSphere Web Client with Windows session authentication (SSPI), you must join the PSC to the Active Directory domain and assign the Administrator role to this user.

One may face issues while trying to join vCSA and PSC to an Active Directory domain unless some prerequisites are configured first. These prerequisites are:

- The user who logs in to the vCenter Server instance in the vCenter Server Appliance is a member of the SystemConfiguration.Administrators group in vCenter Single Sign-On.
- The system name of the appliance is an FQDN. If, during the deployment of the appliance, you set an IP address as a system name, you cannot join the vCenter Server Appliance to an Active Directory domain. Note that the VxRail vCSA and PSC are initialized with FQDNs, and therefore this prerequisite is satisfied by default for VxRail.

Make sure that the DNS server(s) the PSC uses is properly configured and able to resolve the AD Domain Controller before attempting to join the AD domain. As shown in Figure 2 below, the Preferred DNS server IP address can be verified in the Networking page of the PSC.

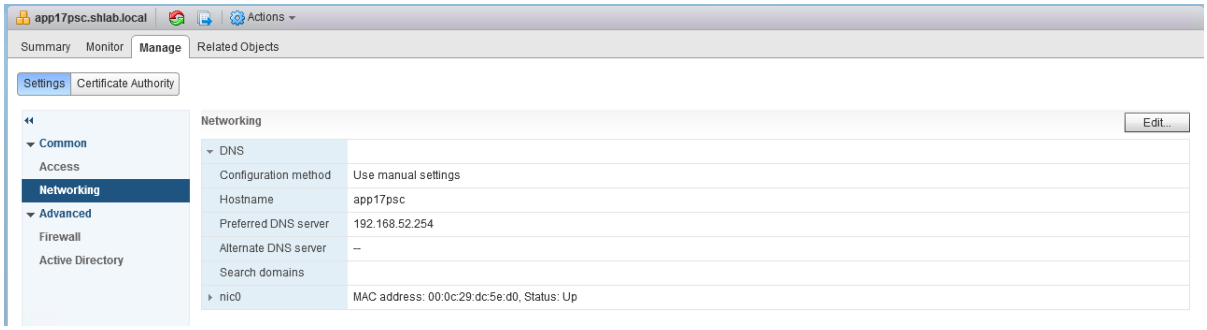

Figure 2 A PSC Appliance Configured within a DNS Server for Name Resolution

Procedure for Joining VxRail PSC to AD – vSphere 6.5

1. Using the vSphere Client, log in to the vCenter Server associated with the Platform Services Controller as a user with administrator privileges in the local vCenter Single Sign-On domain (**vsphere.local** by default).
2. Navigate to **Home > Administration > Deployment > System Configuration**

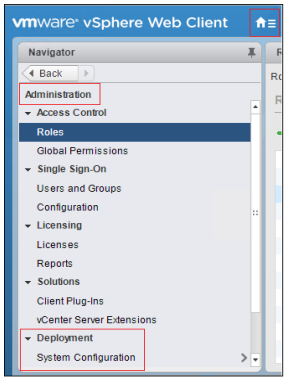

Figure 3 Navigation Steps

3. Under **System Configuration** click **Nodes**, and then select the **PSC** node listed under **Nodes**.

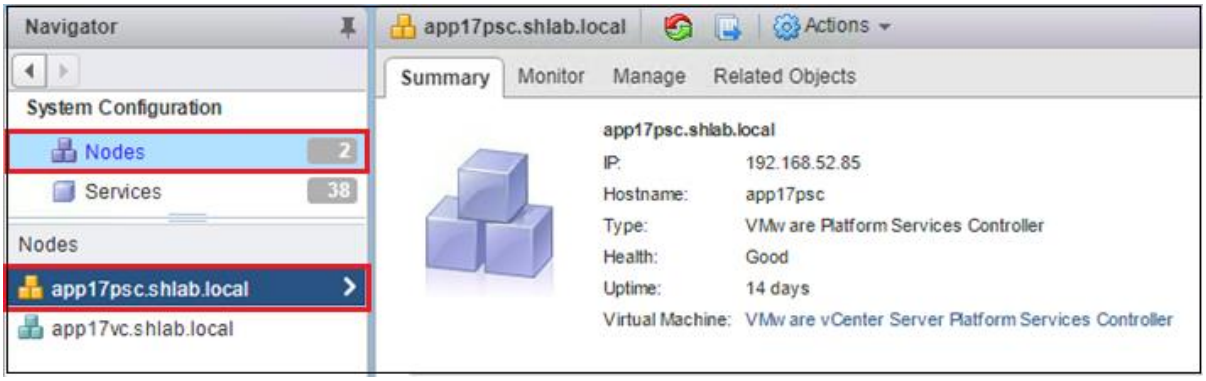

Figure 4 **Selecting PSC from listed nodes**

4. Click **Manage** tab. Under **Advanced**, select **Active Directory**, then click **Join** button.

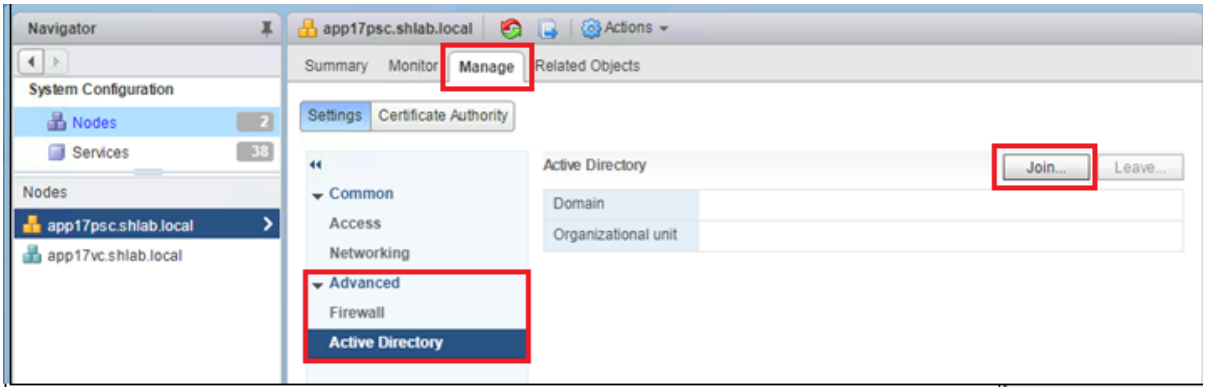

Figure 5 **Selecting PSC and Joining AD**

5. In **Join Active Directory** pop-up box, enter the Active Directory details.

   IMPORTANT: Note that the **User name:** specified here must be in the User Principal Name (UPN) format for both vSphere Web Client and vSphere HTML5 Client; for example, **jchin@mydomain.com**. The down-level logon name format, specifying a domain and a user account in that domain, for example, DOMAIN\UserName, is unsupported.

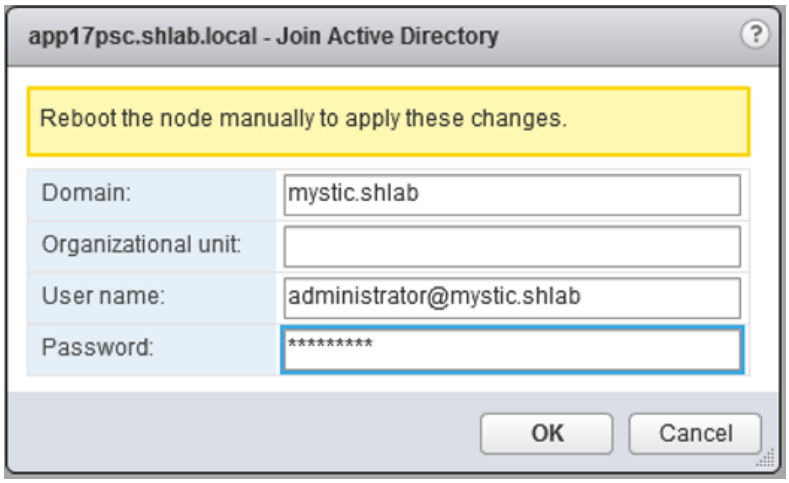

Figure 6 **Join Active Directory window to enter AD details**

6. Click **OK** to join the PSC to the Active Directory domain.
7. Right-click the **PSC** node and select **Reboot** to restart the PSC so that the changes are applied.

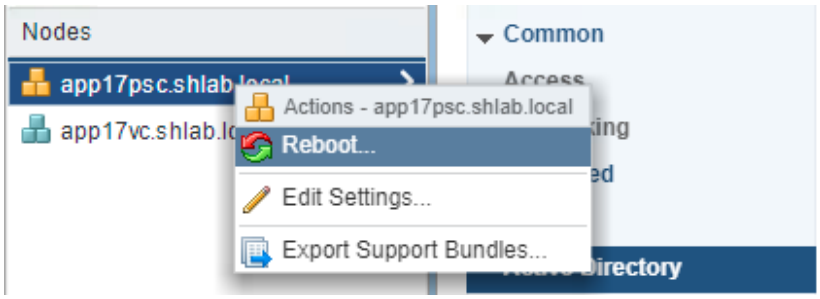

Figure 7 Reboot PSC

Procedure for Joining VxRail PSC to AD – vSphere 6.7

1. Using the vSphere Client, log in to the vCenter Server associated with the Platform Services Controller as a user with administrator privileges in the local vCenter Single Sign-On domain (`vsphere.local` by default).

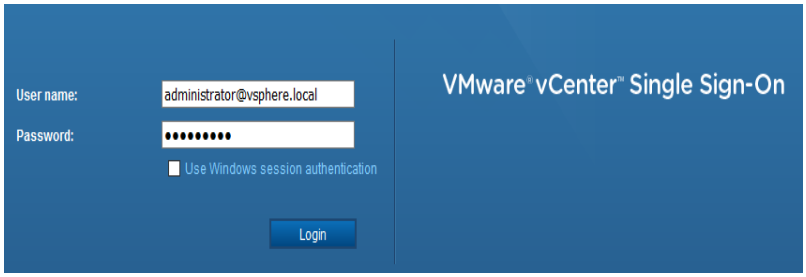

Figure 8 Login Screen

2. Navigate to **Administration > Single Sign On > Configuration**

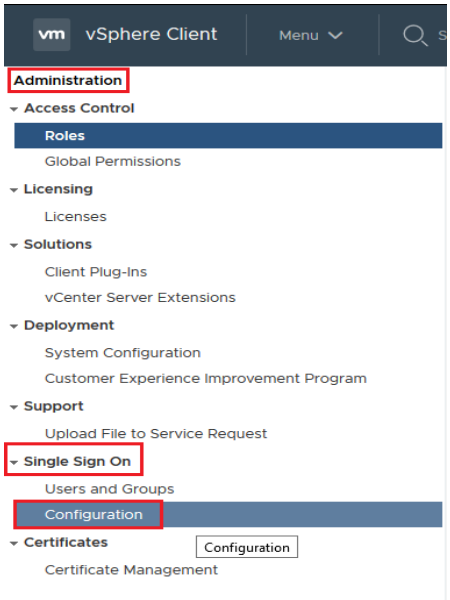

Figure 9 Navigation Steps

3. Click **Active Directory Domain**, and then click **Join AD**

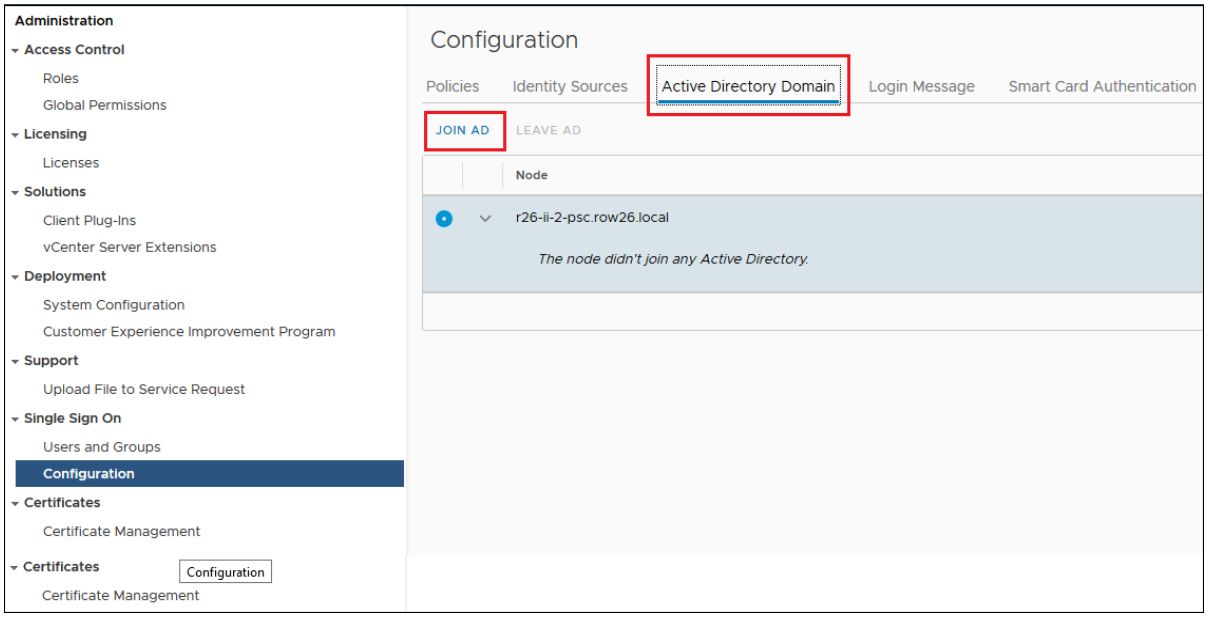

Figure 10 Joining AD

4. In **Join Active Directory Domain** pop-up box, enter the Active Directory details.

   IMPORTANT: Note that the **User name:** specified here must be in the User Principal Name (UPN) format for both vSphere Web Client and vSphere HTML5 Client; for example, **jchin@mydomain.com**. The down-level logon name format, specifying a domain and a user account in that domain, for example, DOMAIN\UserName, is unsupported.

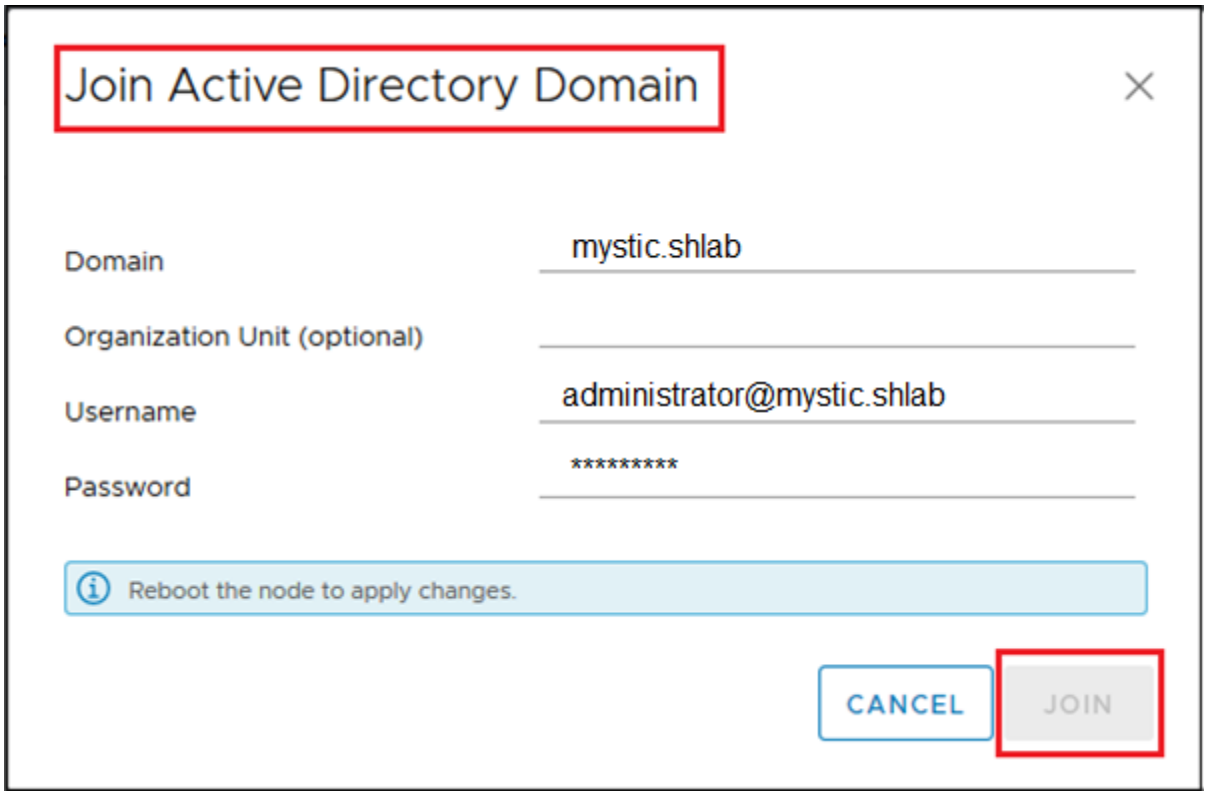

Figure 11 Join Active Directory Domain window to enter AD details

5. Click **JOIN** to join the PSC to the Active Directory domain
6. Navigate to the **PSC** VM and **Restart** the PSC so that the changes are applied.

Verification of the Join Operation

vSphere Client does not provide a clear confirmation message as to whether the operation to join AD has been successful or not. To verify, you can login to AD with required authentication. If the operation to join AD has been successful, you will see the PSC listed in the **Active Directory Users and Computers**.

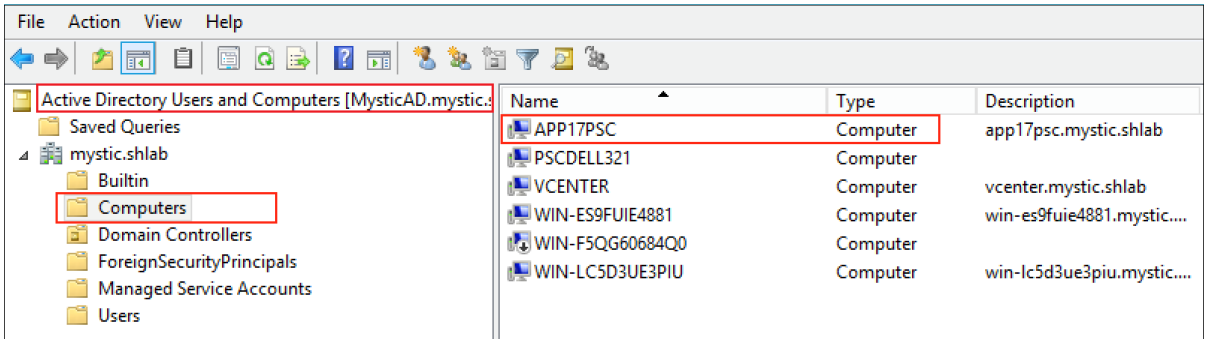

Figure 12 Active Directory Users and Computers must show the PSC

Adding Identity Sources and Assigning Permissions to AD Users

In order for the AD users to be able to login to the VxRail vCenter Server, necessary permissions must be assigned to the AD users. Once the PSC comes up with all its services running properly after it was rebooted, Active Directory Identity Sources must be added.

vSphere 6.5

1. Using the vSphere Web Client, log in to the vCenter Server associated with the Platform Services Controller as a user with administrator privileges in the local vCenter Single Sign-On domain.
2. Navigate to **Administration > Single Sign-On > Configuration**
3. Click the **Identity Sources** tab, and then click the **Add Identity Source** icon or tab.

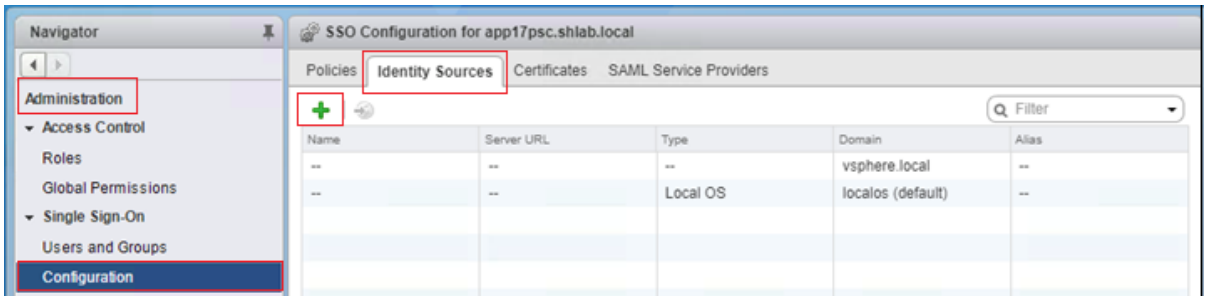

Figure 13 **Navigating to Adding Identity Sources**

4. In the **Add identity source** window, on the **Select Identity Source Type** tab, select **Active Directory (Integrated Windows Authentication)** option and click **Next**.

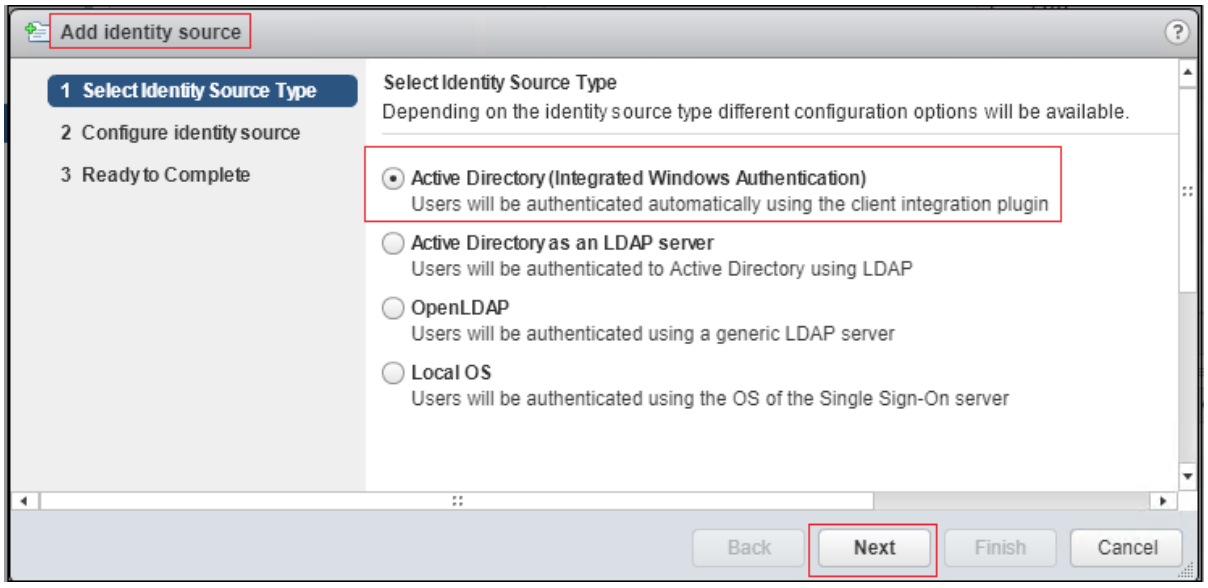

Figure 14 **Add identity source workflow window**

5. On the **Configure Identity source** tab, enter the desired identity source settings of the joined Active Directory domain, and click **Next** (refer to the table below for the descriptions of the settings).

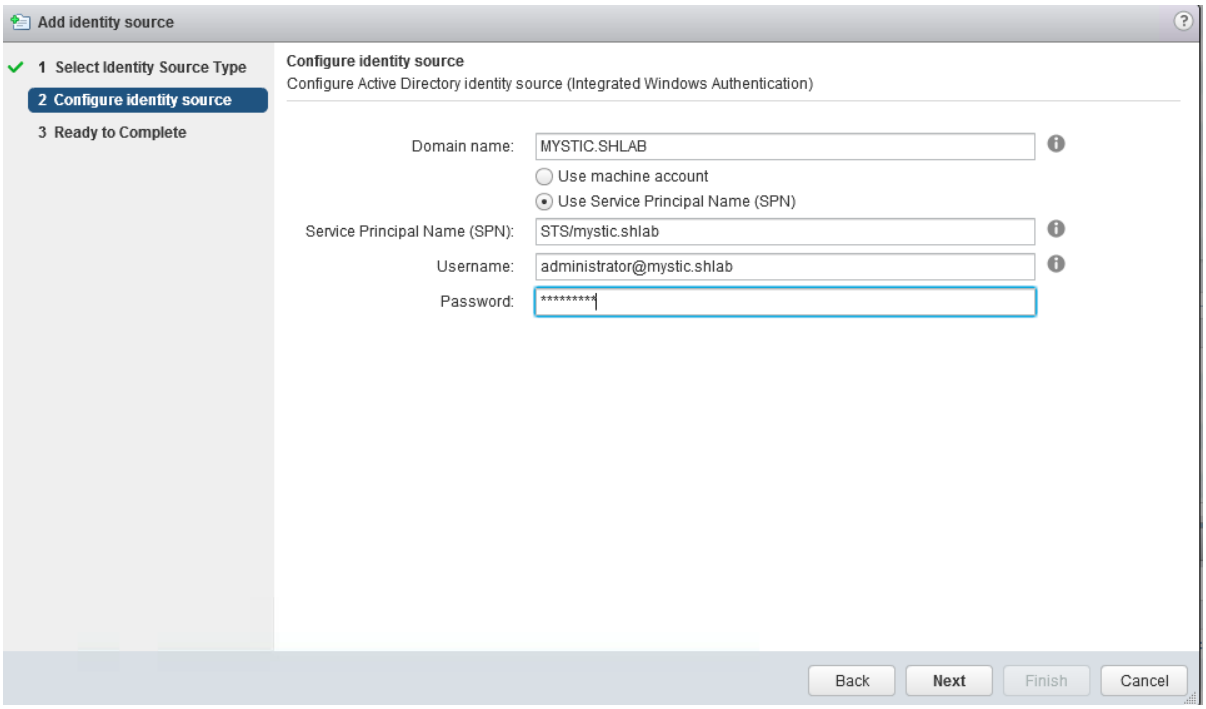

Figure 15 An example identity source configuration using SPN

Text Box	Description
Domain name	FDQN of the domain. Do not provide an IP address in this text box.
Use machine account	Select this option to use the local machine account as the SPN. When you select this option, you specify only the domain name. Do not select this option if you expect to rename this machine.
Use Service Principal Name (SPN)	Select this option if you expect to rename the local machine. You must specify an SPN, a user who can authenticate with the identity source, and a password for the user.
Service Principal Name (SPN)	SPN that helps Kerberos to identify the Active Directory service. Include the domain in the name, for example, STS/example.com. You might have to run **setspn –S** to add the user you want to use. See the Microsoft documentation for information on **setspn**. The SPN must be unique across the domain. Running **setspn –S** checks that no duplicate is created.
User Principal Name (UPN)	Name of a user who can authenticate with this identity source. Use the email address format, for example, jchin@mydomain.com. You can verify the User Principal Name with the Active Directory Service Interfaces Editor (ADSI Edit).
Password	Password for the user who is used to authenticate with this identity source, which is the user who is specified in User Principal Name. Include the domain name, for example, jdoe@example.com.

6. On the **Ready to Complete** tab, review all details and click **Finish**.
7. Verify that you can now see the joined Active Directory domain on the **Identity Sources** tab.
8. Assign the **Administrator Role** to desired **AD user**.

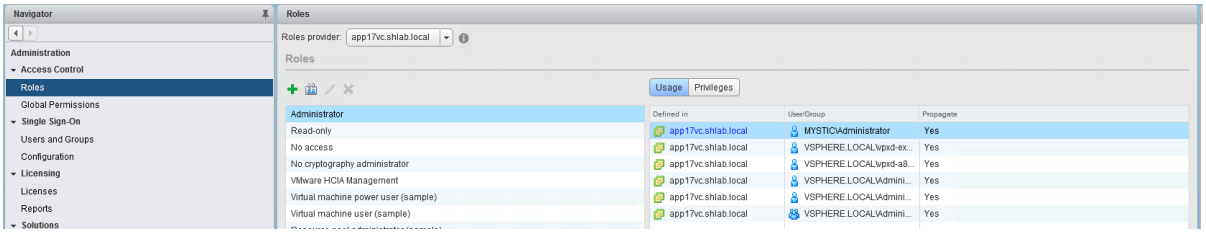

Figure 16 Manipulating Permissions for an AD User

9. Log into vCenter Server via vSphere Web Client with the **AD User**. Once this login is successful, the user should be able to login to the VxRail Manager.
10. Verify that you can log into VxRail Manager using the **AD User** and that the VxRail Manager works properly.

vSphere 6.7

1. Using the vSphere Client, log in to the vCenter Server associated with the Platform Services Controller as a user with administrator privileges in the local vCenter Single Sign-On domain.
2. Navigate to **Administration > Single Sign-On > Configuration**
3. Click the **Identity Sources** tab, and then click the **Add Identity Source** icon or tab

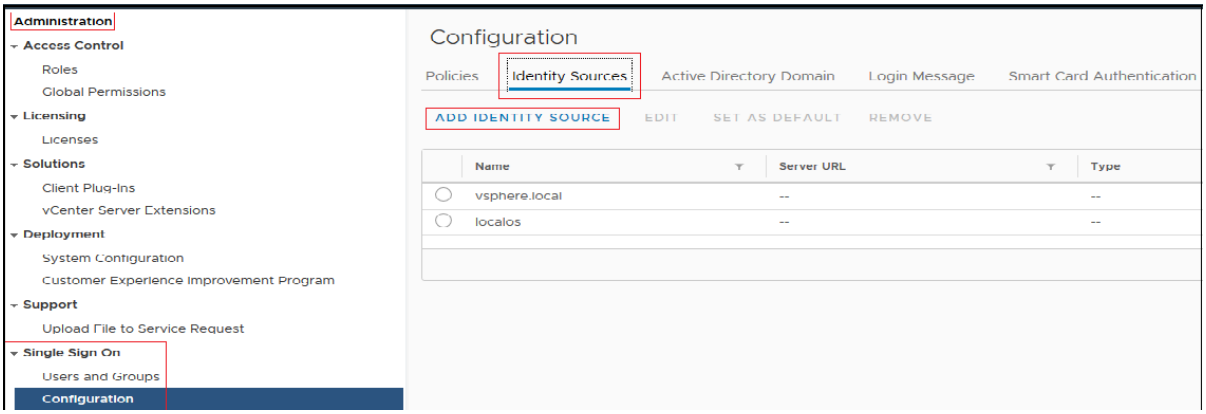

Figure 17 Navigating to Adding Identity Sources

4. In the **Add Identity Source** window, under the **Select Identity Source Type** options, select **Active Directory (Integrated Windows Authentication)** option.

Figure 18 Selecting Identity source type

5. In the **Add Identity Source** window, enter the desired identity source settings of the joined Active Directory domain, and click **ADD** (refer to the table below for the descriptions of the settings).

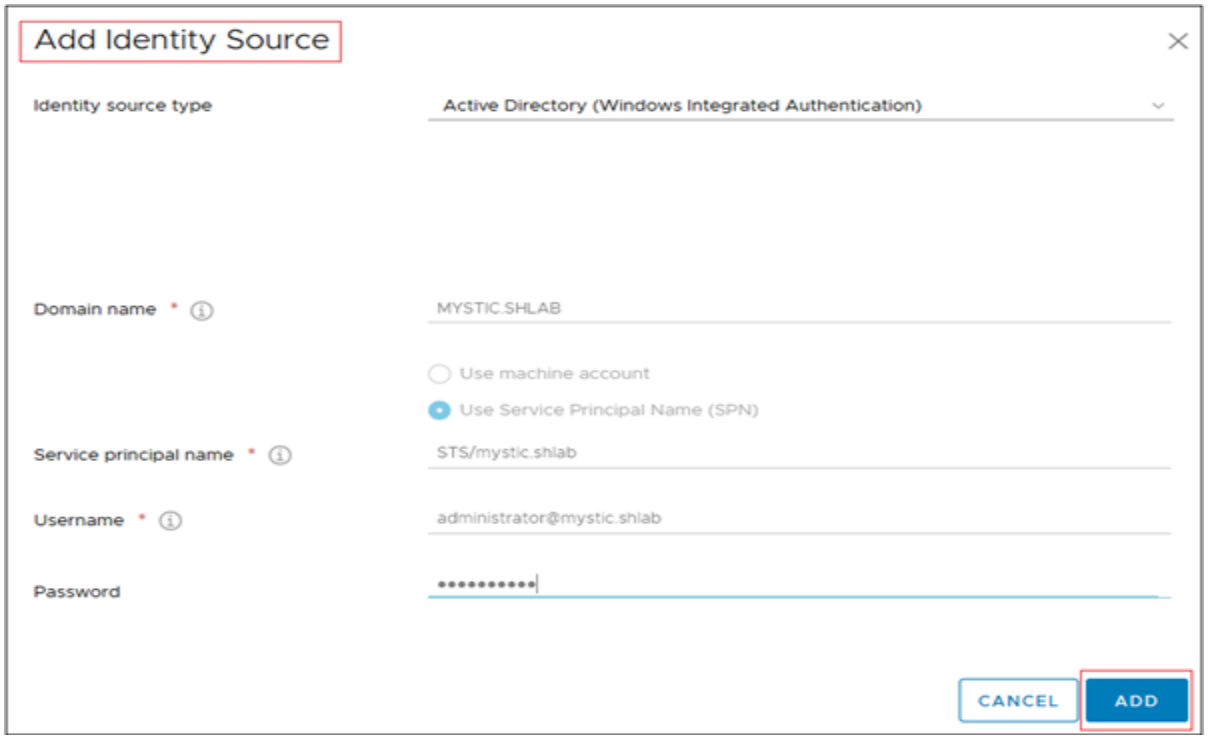

Figure 19 **An example identity source configuration using SPN**

Text Box	Description
Domain name	FDQN of the domain. Do not provide an IP address in this text box.
Use machine account	Select this option to use the local machine account as the SPN. When you select this option, you specify only the domain name. Do not select this option if you expect to rename this machine.
Use Service Principal Name (SPN)	Select this option if you expect to rename the local machine. You must specify an SPN, a user who can authenticate with the identity source, and a password for the user.
Service Principal Name (SPN)	SPN that helps Kerberos to identify the Active Directory service. Include the domain in the name, for example, STS/example.com. You might have to run **setspn –S** to add the user you want to use. See the Microsoft documentation for information on **setspn**. The SPN must be unique across the domain. Running **setspn –S** checks that no duplicate is created.
User Principal Name (UPN)	Name of a user who can authenticate with this identity source. Use the email address format, for example, jchin@mydomain.com. You can verify the User Principal Name with the Active Directory Service Interfaces Editor (ADSI Edit).
Password	Password for the user who is used to authenticate with this identity source, which is the user who is specified in User Principal Name. Include the domain name, for example, jdoe@example.com.

6. Verify that you can now see the joined Active Directory domain on the **Identity Sources** tab.
7. Assign the **Administrator Role** to desired **AD user**.

Figure 20 Manipulating Permissions for an AD User

8. Log into vCenter Server via vSphere Client with the **AD User**. Once this login is successful, the user should be able to login to the VxRail Manager.
9. Verify that you can log into VxRail Manager using the **AD User** and that the VxRail Manager works properly.

Impact of VxRail Upgrades

If a VxRail Supplied PSC has already joined to an AD domain, you might run into an issue when the AD user tries to login the VxRail vCenter Server after a VxRail upgrade. It is possible that a new VxRail Supplied vCSA VM and PSC VM are deployed during the upgrade. That means new guest OS's are running on these VMs. When AD users attempt to login to vCenter Server, they might experience errors. If that happens, the solution would be to remove the PSC from the Active Directory domain and then rejoin PSC to the AD domain.

Conclusion

Joining the VxRail Supplied vCSA and PSC to an Active Directory domain and assigning users and groups from the Active Directory domain to the vCenter Single Sign-On domain are important and error-prone operations. It requires not only very strong skills in vSphere/vCenter administration but also a good understanding of services such as Active Directory Domain Services, Domain Name System and Time Synchronization via Network Time Protocol.

The procedure for joining the VxRail Supplied vCenter Server Appliance (vCSA) and Platform Services Controller (PSC) to an Active Directory domain is described. Moreover, the procedure for attaching the users and groups from this Active Directory domain to the vCenter Single Sign-On domain is included as well. The descriptions adopted a prescriptive step-by-step approach so that they can be easily performed. Due to the prescriptive nature of the procedures and some minor differences between vSphere 6.5 and vSphere 6.7, the procedures are presented separately for these two versions, further facilitating ease of execution of these procedures.

References

- Active Directory Domain Services Overview:

  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

- Install Active Directory Domain Services:

  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100-#BKMK_GUI

- The Machine SID Duplication Myth (and Why Sysprep Matters):

  https://blogs.technet.microsoft.com/markrussinovich/2009/11/03/the-machine-sid-duplication-myth-and-why-sysprep-matters/

- Creating a DNS Infrastructure Design:

  https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/creating-a-dns-infrastructure-design

- DNS Requirements for the vCenter Server Appliance and Platform Services Controller Appliance:

  https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vcenter.install.doc/GUID-24D34C53-B00E-47B7-92A7-6B0155DF6889.html

- DNS domain namespace and AD domain namespace (VMware reference)

  https://docs.vmware.com/en/VMware-vSphere/6.5/rn/vsphere-vcenter-server-651-release-notes.html

- DNS domain namespace and AD domain namespace (Microsoft reference)

  https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc757136%28v%3dws.10%29

- Synchronizing Clocks on the vSphere Networks:

  https://docs.vmware.com/en/VMware-vSphere/6.7/com.vmware.vcenter.install.doc/GUID-9FD3A5E3-6C2D-4161-9270-4BF57FADCE6D.html

- Timekeeping best practices for Windows, including NTP:

  http://kb.vmware.com/kb/1318

- vSphere Single Host Management:

  https://docs.vmware.com/en/VMware-vSphere/6.5/vsphere-html-host-client-18-guide.pdf

- Join the vCenter Server Appliance to an Active Directory Domain:

  https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.vcsa.doc/GUID-08EA2F92-78A7-4EFF-880E-2B63ACC962F3.html

- vSphere Permissions and User Management Tasks:

  https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.security.doc/GUID-5372F580-5C23-4E9C-8A4E-EF1B4DD9033E.html

- Platform Services Controller Administration Guide:

  https://docs.vmware.com/en/VMware-vSphere/6.7/vsphere-esxi-vcenter-server-67-platform-services-controller-administration-guide.pdf

- vSphere Security:

  https://docs.vmware.com/en/VMware-vSphere/6.5/vsphere-esxi-vcenter-server-651-security-guide.pdf

- EMC KB 488890 Issue #13: Upgrade failure using Active Directory account due to username truncated if VC has AD server as Identity Source.

  Workaround: When executing the upgrade task in VxRail Manager, a window titled "VxRail Upgrade requires permission to execute" pops up, asking for vCSA SSO login and VxRail Manager root account. Use "user@domain" instead of "user@domain.local" for vCSA SSO account to execute the upgrade.