COMPONENT DESIGN:
VMWARE IDENTITY MANAGER ARCHITECTURE
Table of Contents

Component Design: VMware Identity Manager Architecture

- Design Overview
- VMware Identity Manager Connector
- Connector Sizing and Availability
- VMware Identity Manager Tenant Installation and Initial Configuration
- VMware Identity Manager Connector Installation and Configuration
- Access to Resources Through VMware Identity Manager
VMware Identity Manager™ is a key component of VMware Workspace ONE®. Among the capabilities of VMware Identity Manager are:

- **Simple application access for end users** – Provides access to different types of applications, including SaaS-based web applications (such as Salesforce, Dropbox, Concur, and many others), native mobile apps, VMware Horizon®-based applications and desktops, RDSH-published applications and desktops, VMware ThinApp® packaged apps, and Citrix-based applications and desktops, all through a unified application catalog.

- **Self-service app store** – Allows end users to search for and select entitled applications in a simple way, while providing enterprise security and compliance controls to ensure that the right users have access to the right applications.

Users can customize the Bookmarks tab for fast, easy access to frequently used applications, and place the apps in a preferred order. IT can optionally push entries onto the Bookmarks tab using automated application entitlements.

- **Enterprise single sign-on (SSO)** – Simplifies business mobility with an included identity provider (IdP) or integration with existing on-premises identity providers so that you can aggregate SaaS, native mobile, and Windows 10 apps into a single catalog. Users have a single identity regardless of whether they log in to an internal, external, or virtual-based application.

- **Conditional access** – Includes a comprehensive policy engine that allows the administrator to set different access policies based upon the risk profile of the application. An administrator can use criteria, such as network range, user group, application type, or device operating system, to determine how authentication is done for the user.

In addition, VMware Identity Manager has the ability to validate the compliance status of the device in VMware Workspace ONE® UEM (powered by AirWatch). Failure to meet the compliance standards blocks a user from signing in to an application or accessing applications in the catalog until the device becomes compliant.

- **Enterprise identity management with adaptive access** – Establishes trust between users, devices, and the hybrid cloud for a seamless user experience and powerful conditional access.
controls that leverage Workspace ONE UEM device enrollment and SSO adapters.

- **Workspace ONE native mobile apps** – Includes native apps for iOS, Android, and Windows 10, to simplify finding, installing enterprise apps, and providing an SSO experience across resource types.

**Figure**: User Workspace Delivered by VMware Identity Manager

**Design Overview**

VMware Identity Manager can be implemented using either an on-premises or a cloud-based (SaaS) implementation model.

In a cloud-based implementation, a VMware Identity Manager Connector service synchronizes user accounts from Active Directory to the VMware Identity Manager tenant service. Applications can then be accessed from a cloud-based entry point.

VMware Identity Manager can also be integrated with VMware Horizon® Cloud Service™ to provide access to Horizon desktops and published applications. The VMware Identity Manager tenant handles authentication and provides SSO services to applications and desktops.

**Design decision**: In this reference architecture, a cloud-based VMware Identity Manager instance was used.
The main components of a VMware Identity Manager cloud-based implementation are:

- **VMware Identity Manager tenant** – Hosted in cloud and runs the main VMware Identity Manager service.

- **VMware Identity Manager Connector** – Responsible for directory synchronization and authentication between on-premises resources such as Active Directory, VMware Horizon, and the VMware Identity Manager service. You can deploy the connector by running the Windows-based installer.

**VMware Identity Manager Connector**

The VMware Identity Manager Connector can synchronize resources such as Active Directory, Horizon Cloud, and VMware Horizon® 7. The connector can run inside the LAN in outbound-only connection mode, meaning the connector receives no incoming connections from the DMZ.

Whereas the VMware AirWatch® Cloud Connector (ACC) facilitates AD/ LDAP integration with Workspace ONE, the VMware Identity Manager Connector allows AD/ LDAP integration with VMware Identity Manager.

Deploying a VMware Identity Manager Connector provides the following capabilities:

- VMware Identity Manager Connector–based authentication methods such as password, RSA Adaptive Authentication, RSA SecurID, and RADIUS
- Kerberos authentication for internal users
- Integration with the following resources:
  - On-premises Horizon 7 desktop and application pools
  - Horizon Cloud Service desktops and applications
  - Citrix-published resources

There are several similarities between the VMware Identity Manager Connector and the AirWatch Cloud Connector:
Both connectors synchronize with an enterprise directory (Active Directory/ LDAP) to import directory users to Workspace ONE components.

Both the VMware Identity Manager Connector and the AirWatch Cloud Connector are Windows services. They can be installed on separate servers or on the same Windows Server.

The VMware Identity Manager Connector can be deployed in an outbound-only mode like the AirWatch Cloud Connector. This removes any requirements for organizations to change their inbound firewall rules and configurations.

Similar to the AirWatch Cloud Connector, the VMware Identity Manager traffic is balanced by AirWatch Cloud Messaging (AWCM).

Differences:

- The VMware Identity Manager Connector is required when synchronizing VMware Horizon resources, such as Horizon 7 or Horizon Cloud.

- Although the AirWatch Cloud Connector provides directory authentication for Workspace ONE, the VMware Identity Manager Connector provides a wider range of authentication mechanisms, such as RSA Adaptive Authentication, RSA SecurID, RADIUS, and Kerberos.

The VMware Identity Manager Connector and the AirWatch Cloud Connector have complementary purposes. Depending on the requirements, you might choose to install only the ACC component or both the ACC and the VMware Identity Manager Connector. For customers looking to implement the Workspace ONE solution, it is recommended to install both.

The VMware Identity Manager Connector and the AirWatch Cloud Connector can be installed on the same Windows Server instance or on separate server instances. If both components are co-located, give the server instance sufficient hardware resources to cope with the combined load.

**Design decision:** For this reference architecture, the VMware Identity Manager Connector was deployed to support the requirements of VMware Identity Manager directory integration and to allow a wide range of authentication methods. This connector also enabled synchronization of resources from Horizon Cloud Service on Microsoft Azure into the Workspace ONE catalog.

**Connector Sizing and Availability**

VMware Identity Manager Connector can be setup for high availability and failover by adding multiple connector instances in a cluster. If one of the connector instances becomes unavailable for any reason, other instances will still be available.

To create a cluster, you install new connector instances and configure them in exactly the same way as you set up the first connector. You then associate all the connector instances with the built-in identity provider. The VMware Identity Manager service automatically distributes traffic among all the connectors associated with the built-in identity providers so that you do not need an external load balancer. If one of the connectors becomes unavailable, the service does not direct traffic to it until connectivity is restored.
See Configuring High Availability for the VMware Identity Manager Connector in VMware Identity Manager Cloud Deployment for more detail.

After you set up the connector cluster, the authentication methods that you have enabled on the connector are highly available. If one of the connector instances becomes unavailable, authentication is still available. However, directory sync can be enabled on only one connector at a time, and you must modify the directory settings in the VMware Identity Manager service to use another connector instance instead of the original connector instance. For instructions, see Enabling Directory Sync on Another Connector in the Event of a Failure in VMware Identity Manager Cloud Deployment.

Sizing guidance for the recommended number of VMware Identity Manager Connectors is given in the On-Premises Architecture Hardware Assumptions section of the VMware Workspace ONE UEM Recommended Architecture Guide or the ARCHITECTURE section of the VMware Workspace ONE UEM Online Help. The documentation also includes the recommended hardware specification. Note that the documentation shows only the number connectors required for each sizing scenario to cope with the load demand. It does not include additional servers in those numbers to account for redundancy.

**Design decision:** Three instances of the VMware Identity Manager Connectors were deployed. Two were required based on load, and a third was added for redundancy.

**VMware Identity Manager Tenant Installation and Initial Configuration**

Because the VMware Identity Manager tenant is cloud-based, you do not have to make design decisions with regards to database, network access, or storage considerations. The VMware Identity Manager service scales to accommodate virtually any size of organization.

Connectivity to the VMware Identity Manager service is through outbound port 443. This connection is used for directory synchronization, authentication, and syncing entitlements for resources, such as Horizon desktops and apps. Organizations can take advantage of this configuration with no additional inbound firewall ports opened to the Internet.

Initial configuration involves logging in to the VMware Identity Manager service with the provided credentials at a URL similar to `https://<company>.vmwareidentity.com`.

For more information, see the VMware Identity Manager Cloud Documentation.

**Next Steps**

To leverage the breadth of the Workspace ONE experience, you must integrate Workspace ONE UEM and VMware Identity Manager into Workspace ONE. After integration:

- Workspace ONE can use VMware Identity Manager for authentication and access to SaaS and VMware Horizon applications.
- Workspace ONE can use Workspace ONE UEM for device enrollment and management.

See Integrating Workspace ONE UEM With VMware Identity Manager in the Guide to Deploying VMware Workspace ONE with VMware Identity Manager.
VMware Identity Manager Connector Installation and Configuration

For prerequisites, including system and network configuration requirements, see *Preparing to Install VMware Identity Manager Connector* in the VMware Identity Manager Cloud Deployment documentation.

For installation instructions, see the *Deploying the VMware Identity Manager Connector* section of the VMware Identity Manager Cloud Deployment documentation.

Be sure to deploy the VMware Identity Manager Connector in outbound-only mode. This removes any requirements for organizations to change their inbound firewall rules and configurations. See *Enable Outbound Mode for the VMware Identity Manager Connector* in VMware Identity Manager Cloud Deployment.

Access to Resources Through VMware Identity Manager

VMware Identity Manager powers the Workspace ONE catalog, providing self-service access to company applications for business users. VMware Identity Manager is responsible for the integration with web-based SaaS applications, internal web applications, ThinApp-packaged apps, and VMware Horizon for the delivery of virtual desktops and published applications. All of these desktops and apps are displayed to the user in the catalog based on directory entitlements.

Based on the types of applications to be delivered to end users, the catalog is configured to integrate with the relevant services.

Workspace ONE Native Mobile Apps

For many users, their first experience with Workspace ONE is likely through the Workspace ONE native mobile app. The Workspace ONE app provides the user a branded self-service catalog to access their corporate resources. The catalog provides the necessary applications for the user to do their job, and also offers access to other company resources, such as a company directory lookup. Native operating features, such as Apple Touch ID on an iOS device or Windows Hello on Windows 10, can be used to enhance the user experience.

The Workspace ONE app:

- Delivers a unified application catalog of web, mobile, and virtual applications to the user. This is provided through an integration that aggregates VMware Identity Manager applications with Workspace ONE UEM–delivered applications.
- Provides a launcher to access SaaS apps, Horizon virtual desktops and apps, and ThinApp-packaged apps, to give a consolidated and consistent way of discovering and launching all types of applications.
- Gives the user the ability to search across an enterprise’s entire deployment of application resources.
- Offers SSO technology for simple user access to resources without requiring users to remember each site’s password.
The Workspace ONE native app is available from the various app stores and can be deployed through Workspace ONE UEM as part of a device enrollment process.

SaaS Apps

SaaS applications, such as Concur and Salesforce, are often authenticated through federation standards, such as Security Assertion Markup Language (SAML) or Web Services Federation (WSFed), to offload authentication to an identity provider. Often browser-based, these applications are published through VMware Identity Manager. The cloud application catalog in VMware Identity Manager includes templates with many preconfigured parameters to make federating with the SaaS provider easier. For SaaS providers where there is no template, a wizard guides you through configuring the application and entitling users.
Figure: Administrator Adding a New SaaS Application to the Catalog
OpenID Connect (OIDC) is the preferred method for single sign-on (SSO) with modern web applications (and also native mobile applications). It allows an end user with a browser to log into an Identity Provider (IdP) such as VMware Identity Manager using JSON-based communication.

Refer the section Adding OpenID Connect Applications to the Catalog in Setting Up Resources in VMware Identity Manager (Cloud) for more details on how to manage OpenID applications with the Workspace ONE catalog.

VMware Horizon Apps and Desktops

The capability to deliver virtual apps and desktops continues to be a significant value for Workspace ONE users. VMware Identity Manager can be integrated with a VMware Horizon implementation to expose the entitled apps and desktops to end users. Through VMware Horizon® Client™ for native mobile platforms, access to these resources can be easily extended to mobile devices.

You must deploy the VMware Identity Manager Connector to provide access to Horizon resources from the VMware Identity Manager cloud-hosted service. The connector enables you to synchronize entitlements to the service. To allow users to access Horizon resources from the Internet, you must
deploy VMware Unified Access Gateway™ as part of the Horizon solution.

See *Integrate Horizon Cloud Service with VMware Identity Manager* in the Platform Integration section of this guide.

**ThinApp-Packaged Apps**

ThinApp is a Windows application virtualization solution that can accelerate deployment by isolating applications from the underlying operating system to eliminate application conflict. Apps that are packaged with ThinApp can be distributed from file shares in the enterprise. In a Workspace ONE implementation, ThinApp packages can be published to Windows-based systems through VMware Identity Manager and deployed to physical or virtual machines. The VMware Identity Manager Connector must be deployed to enable using ThinApp-packaged apps in a Workspace ONE deployment.

See *Providing Access to VMware ThinApp Packages* in *Setting Up Resources in VMware Identity Manager (Cloud)*.