Directory Integration with VMware Identity Manager

DEC 2017
VMware AirWatch 9.2
VMware Identity Manager 3.1

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Directory Integration with VMware Identity Manager

Directory Integration with VMware Identity Manager provides information about integrating your enterprise directory with VMware Identity Manager™ to sync users and groups to the VMware Identity Manager service.

Intended Audience

This information is intended for experienced Windows or Linux system administrators who are familiar with Active Directory and other directory services.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Integrating Your Enterprise Directory with VMware Identity Manager

1

You integrate your enterprise directory with VMware Identity Manager to sync users and groups from your enterprise directory to the VMware Identity Manager service.

The following types of directories are supported.

- Active Directory over LDAP
- Active Directory, Integrated Windows Authentication
- LDAP directory

To integrate your enterprise directory, you perform the following tasks.

- Specify the attributes that you want users to have in the VMware Identity Manager service.
- Create a directory in the VMware Identity Manager service of the same type as your enterprise directory and specify the connection details.
- Map the VMware Identity Manager attributes to attributes used in your Active Directory or LDAP directory.
- Specify the users and groups to sync.
- Sync users and groups.

After you integrate your enterprise directory and perform the initial sync, you can update the configuration, set up a sync schedule to sync regularly, or start a sync at any time.

Important Concepts Related to Directory Integration 2

Several concepts are integral to understanding how the VMware Identity Manager service integrates with your Active Directory or LDAP directory environment.

VMware Identity Manager Connector

The VMware Identity Manager Connector is a component of the VMware Identity Manager service. In an on-premises VMware Identity Manager instance, a connector is already embedded in the service. In a SaaS deployment, you deploy the connector on premises inside your enterprise network.

- Syncs user and group data from your Active Directory or LDAP directory to the VMware Identity Manager service.
- When being used as an identity provider, authenticates users to the VMware Identity Manager service.

  The connector is the default identity provider. You can also use third-party identity providers that support the SAML 2.0 protocol. Use a third-party identity provider for an authentication type the connector does not support, or if the third-party identity provider is preferable based on your enterprise security policy.

  Note If you use third-party identity providers, you can either configure the connector to sync user and group data or configure Just-in-Time user provisioning. See the Just-in-Time User Provisioning section in *VMware Identity Manager Administration* for more information.

Directory

The VMware Identity Manager service has its own concept of a directory, corresponding to the Active Directory or LDAP directory in your environment. This directory uses attributes to define users and groups. You create one or more directories in the service and then sync those directories with your Active Directory or LDAP directory. You can create the following directory types in the service.

- Active Directory
  - Active Directory over LDAP. Create this directory type if you plan to connect to a single Active Directory domain environment. For the Active Directory over LDAP directory type, the connector binds to Active Directory using simple bind authentication.

- Active Directory, Integrated Windows Authentication. Create this directory type if you plan to connect to a multi-domain or multi-forest Active Directory environment. The connector binds to Active Directory using Integrated Windows Authentication.

  The type and number of directories that you create varies depending on your Active Directory environment, such as single domain or multi-domain, and on the type of trust used between domains. In most environments, you create one directory.

- LDAP Directory

The service does not have direct access to your Active Directory or LDAP directory. Only the connector has direct access. Therefore, you associate each directory created in the service with a connector instance.

Worker

When you associate a directory with a connector instance, the connector creates a partition for the associated directory called a worker. A connector instance can have multiple workers associated with it. Each worker acts as an identity provider. You define and configure authentication methods per worker.

The connector syncs user and group data between your Active Directory or LDAP directory and the service through one or more workers.

Important You cannot have two workers of the Active Directory, Integrated Windows Authentication type on the same connector instance.

Security Considerations

For enterprise directories integrated with the VMware Identity Manager service, security settings such as user password complexity rules and account lockout policies must be set in the enterprise directory directly. VMware Identity Manager does not override these settings.

Integrating with Active Directory

3

You can integrate VMware Identity Manager with your Active Directory deployment to sync users and groups from Active Directory to VMware Identity Manager.

See also Chapter 2 Important Concepts Related to Directory Integration.

This section includes the following topics:

- Active Directory Environments
- About Domain Controller Selection (domain_krb.properties file)
- Managing User Attributes that Sync from Active Directory
- Permissions Required for Joining a Domain (Linux Virtual Appliance Only)
- Configuring Active Directory Connection to the Service
- Enabling Users to Change Active Directory Passwords
- Setting up Directory Sync Safeguards

Active Directory Environments

You can integrate the service with an Active Directory environment that consists of a single Active Directory domain, multiple domains in a single Active Directory forest, or multiple domains across multiple Active Directory forests.

Single Active Directory Domain Environment

A single Active Directory deployment allows you to sync users and groups from a single Active Directory domain.

For this environment, when you add a directory to the service, select the Active Directory over LDAP option.

For more information, see:

- About Domain Controller Selection (domain_krb.properties file)
- Managing User Attributes that Sync from Active Directory
- Configuring Active Directory Connection to the Service

Multi-Domain, Single Forest Active Directory Environment

A multi-domain, single forest Active Directory deployment allows you to sync users and groups from multiple Active Directory domains within a single forest.

You can configure the service for this Active Directory environment as a single Active Directory, Integrated Windows Authentication directory type or, alternatively, as an Active Directory over LDAP directory type configured with the global catalog option.

- The recommended option is to create a single Active Directory, Integrated Windows Authentication directory type.

  When you add a directory for this environment, select the Active Directory (Integrated Windows Authentication) option.

  For more information, see:

  - About Domain Controller Selection (domain_krb.properties file)
  - Managing User Attributes that Sync from Active Directory
  - Configuring Active Directory Connection to the Service

- If Integrated Windows Authentication does not work in your Active Directory environment, create an Active Directory over LDAP directory type and select the global catalog option.

  Some of the limitations with selecting the global catalog option include:

  - The Active Directory object attributes that are replicated to the global catalog are identified in the Active Directory schema as the partial attribute set (PAS). Only these attributes are available for attribute mapping by the service. If necessary, edit the schema to add or remove attributes that are stored in the global catalog.
  - The global catalog stores the group membership (the member attribute) of only universal groups. Only universal groups are synced to the service. If necessary, change the scope of a group from a local domain or global to universal.
  - The bind DN account that you define when configuring a directory in the service must have permissions to read the Token-Groups-Global-And-Universal (TGGAU) attribute.
  - When AirWatch is integrated with VMware Identity Manager and multiple AirWatch organization groups are configured, the Active Directory Global Catalog option cannot be used.

  Active Directory uses ports 389 and 636 for standard LDAP queries. For global catalog queries, ports 3268 and 3269 are used.

  When you add a directory for the global catalog environment, specify the following during the configuration.

  - Select the Active Directory over LDAP option.
  - Deselect the check box for the option **This Directory supports DNS Service Location**.

- Select the option **This Directory has a Global Catalog**. When you select this option, the server port number is automatically changed to 3268. Also, because the Base DN is not needed when configuring the global catalog option, the Base DN text box does not display.
- Add the Active Directory server host name.
- If your Active Directory requires access over SSL, select the option **This Directory requires all connections to use SSL** and paste the certificate in the text box provided. When you select this option, the server port number is automatically changed to 3269.

Multi-Forest Active Directory Environment with Trust Relationships

A multi-forest Active Directory deployment with trust relationships allows you to sync users and groups from multiple Active Directory domains across forests where two-way trust exists between the domains.

When you add a directory for this environment, select the Active Directory (Integrated Windows Authentication) option.

For more information, see:

- About Domain Controller Selection (domain_krb.properties file)
- Managing User Attributes that Sync from Active Directory
- Configuring Active Directory Connection to the Service

Multi-Forest Active Directory Environment Without Trust Relationships

A multi-forest Active Directory deployment without trust relationships allows you to sync users and groups from multiple Active Directory domains across forests without a trust relationship between the domains. In this environment, you create multiple directories in the service, one directory for each forest.

The type of directories you create in the service depends on the forest. For forests with multiple domains, select the Active Directory (Integrated Windows Authentication) option. For a forest with a single domain, select the Active Directory over LDAP option.

For more information, see:

- About Domain Controller Selection (domain_krb.properties file)
- Managing User Attributes that Sync from Active Directory
- Configuring Active Directory Connection to the Service

About Domain Controller Selection (domain_krb.properties file)

The `domain_krb.properties` file determines which domain controllers are used for directories that have DNS Service Location (SRV records) lookup enabled. It contains a list of domain controllers for each domain. The connector creates the file initially, and you must maintain it subsequently. The file overrides DNS Service Location (SRV) lookup.

The following types of directories have DNS Service Location lookup enabled:

- Active Directory over LDAP with the **This Directory supports DNS Service Location** option selected
- Active Directory (Integrated Windows Authentication), which always has DNS Service Location lookup enabled

When you first create a directory that has DNS Service Location lookup enabled, a `domain_krb.properties` file is created automatically and auto-populated with domain controllers for each domain. To populate the file, the connector attempts to find domain controllers that are at the same site as the connector and selects two that are reachable and that respond the fastest.

When you create additional directories that have DNS Service Location enabled, or add new domains to an Integrated Windows Authentication directory, the new domains, and a list of domain controllers for them, are added to the file.

You can override the default selection at any time by editing the `domain_krb.properties` file. As a best practice, after you create a directory, view the `domain_krb.properties` file and verify that the domain controllers listed are the optimal ones for your configuration. For a global Active Directory deployment that has multiple domain controllers across different geographical locations, using a domain controller that is in close proximity to the connector ensures faster communication with Active Directory.

You must also update the file manually for any other changes. The following rules apply.

- The `domain_krb.properties` file is created in the server that contains the connector. A server can only have one `domain_krb.properties` file.

  In a typical on-premises deployment, with no additional connectors deployed, the file is created in the VMware Identity Manager service server. If you are using an external connector for the directory, the file is created in the connector server.

  In a SaaS deployment, the file is created in the connector server.

  In a service or connector Linux virtual appliance, the `domain_krb.properties` file is located in the `/usr/local/horizon/conf` directory. In a service or connector Windows server, the `domain_krb.properties` file is located in the *`installDir`*`\IDMConnector\usr\local\horizon\conf` directory.
- The file is created, and auto-populated with domain controllers for each domain, when you first create a directory that has DNS Service Location lookup enabled.

- Domain controllers for each domain are listed in order of priority. To connect to Active Directory, the connector tries the first domain controller in the list. If it is not reachable, it tries the second one in the list, and so on.
- The file is updated only when you create a new directory that has DNS Service Location lookup enabled or when you add a domain to an Integrated Windows Authentication directory. The new domain and a list of domain controllers for it are added to the file.

  Note that if an entry for a domain already exists in the file, it is not updated. For example, if you created a directory, then deleted it, the original domain entry remains in the file and is not updated.
- The file is not updated automatically in any other scenario. For example, if you delete a directory, the domain entry is not deleted from the file.
- If a domain controller listed in the file is not reachable, edit the file and remove it.
- If you add or edit a domain entry manually, your changes will not be overwritten.

For information on editing the `domain_krb.properties` file, see Editing the domain_krb.properties file.

Important (Linux virtual appliance only) The `/etc/krb5.conf` file must be consistent with the `domain_krb.properties` file. Whenever you update the `domain_krb.properties` file, also update the `krb5.conf` file. See Editing the domain_krb.properties file and Knowledge Base article 2091744 for more information.

How Domain Controllers are Selected to Auto-Populate the domain_krb.properties File

To auto-populate the `domain_krb.properties` file, domain controllers are selected by first determining the subnet on which the connector resides (based on the IP address and netmask), then using the Active Directory configuration to identify the site of that subnet, getting the list of domain controllers for that site, filtering the list for the appropriate domain, and picking the two domain controllers that respond the fastest.

To detect the domain controllers that are the closest, VMware Identity Manager has the following requirements:

- The subnet of the connector must be present in the Active Directory configuration, or a subnet must be specified in the `runtime-config.properties` file. See Overriding the Default Subnet Selection.

  The subnet is used to determine the site.
- The Active Directory configuration must be site aware.

If the subnet cannot be determined or if your Active Directory configuration is not site aware, DNS Service Location lookup is used to find domain controllers, and the file is populated with a few domain controllers that are reachable. Note that these domain controllers may not be at the same geographical location as the connector, which can result in delays or timeouts while communicating with Active Directory. In this case, edit the `domain_krb.properties` file manually and specify the correct domain controllers to use for each domain. See Editing the domain_krb.properties file.

Sample domain_krb.properties File

```
example.com=host1.example.com:389,host2.example.com:389
```

Overriding the Default Subnet Selection

To auto-populate the `domain_krb.properties` file, the connector attempts to find domain controllers that are at the same site so there is minimal latency between the connector and Active Directory.

To find the site, the connector determines the subnet on which it resides, based on its IP address and netmask, then uses the Active Directory configuration to identify the site for that subnet. If the subnet is not in Active Directory, or if you want to override the automatic subnet selection, you can specify a subnet in the `runtime-config.properties` file.

Procedure

1. (Linux virtual appliance) Edit the `/usr/local/horizon/conf/runtime-config.properties` file.
   a. Log in to the virtual machine as the root user.

      For an on premises deployment with no external connectors, log in to the service virtual machine. If you are using an external connector for the directory, log in to the connector virtual machine instead.

      For a SaaS deployment, log in to the connector virtual machine.

   b. Edit the `/usr/local/horizon/conf/runtime-config.properties` file to add the following attribute.

      `siteaware.subnet.override=`*`subnet`*

      where *subnet* is a subnet for the site whose domain controllers you want to use. For example:

      `siteaware.subnet.override=10.100.0.0/20`

2. (Windows server) Edit the `installDir\IDMConnector\usr\local\horizon\conf\runtime-config.properties` file to add the following attribute.

   `siteaware.subnet.override=`*`subnet`*

   where *subnet* is a subnet for the site whose domain controllers you want to use. For example:

   `siteaware.subnet.override=10.100.0.0/20`

3. Save and close the file.
4. Restart the service.

   For a Linux virtual appliance, use this command:

   ```
   service horizon-workspace restart
   ```

Editing the domain_krb.properties file

The `domain_krb.properties` file determines the domain controllers to use for directories that have DNS Service Location lookup enabled. You can edit the file at any time to modify the list of domain controllers for a domain, or to add or delete domain entries. Your changes will not be overridden.

In a Linux virtual appliance, the `domain_krb.properties` file is located in the `/usr/local/horizon/conf` directory. In a Windows server, the `domain_krb.properties` file is located in the *`installDir`*`\IDMConnector\usr\local\horizon\conf` directory.

The file is initially created and auto-populated by the connector. You need to update it manually in some cases, such as the following scenarios.

- If the domain controllers selected by default are not the optimal ones for your configuration, edit the file and specify the domain controllers to use.
- If you delete a directory, delete the corresponding domain entry from the file.
- If any domain controllers in the file are not reachable, remove them from the file.

See also About Domain Controller Selection (domain_krb.properties file).

Procedure

1. (Linux virtual appliance) Log in to the VMware Identity Manager service or connector virtual machine as the root user.

   In a typical on-premises deployment, with no additional connectors deployed, the file is created in the VMware Identity Manager service server. If you are using an external connector for the directory, the file is created in the connector server.

   In a SaaS deployment, the file is created in the connector server.
2. (Windows server) Log in to the VMware Identity Manager service or connector server.

   In a typical on-premises deployment, with no additional connectors deployed, the file is created in the VMware Identity Manager service server. If you are using an external connector for the directory, the file is created in the connector server.

   In a SaaS deployment, the file is created in the connector server.
3. (Linux virtual appliance) Change directories to `/usr/local/horizon/conf`.
4. (Windows server) Go to the *`installDir`*`\IDMConnector\usr\local\horizon\conf` directory.
5. Edit the `domain_krb.properties` file to add or edit the list of domain to host values.

   Use the following format:

   `domain=host:port,host2:port,host3:port`

   For example:

   `example.com=examplehost1.example.com:389,examplehost2.example.com:389`

List the domain controllers in order of priority. To connect to Active Directory, the connector tries the first domain controller in the list. If it is not reachable, it tries the second one in the list, and so on.

Important Domain names must be in lowercase.

6 Change the owner of the `domain_krb.properties` file to `horizon` and group to `www`.

On Linux, use the following command:

```
chown horizon:www /usr/local/horizon/conf/domain_krb.properties
```

7 Restart the service.

On Linux, use the following command:

```
service horizon-workspace restart
```

What to do next

(Linux virtual appliance only) After you edit the `domain_krb.properties` file, edit the `/etc/krb5.conf` file. The `krb5.conf` file must be consistent with the `domain_krb.properties` file.

1 Edit the `/etc/krb5.conf` file and update the `realms` section to specify the same domain-to-host values that are used in the `/usr/local/horizon/conf/domain_krb.properties` file. You do not need to specify the port number. For example, if your `domain_krb.properties` file has the domain entry `example.com=examplehost.example.com:389`, you would update the `krb5.conf` file to the following.

```
[realms]
GAUTO-QA.COM = {
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO-QA\.COM\\.*)s/^GAUTO-QA\.COM/GAUTO-QA/
auth_to_local = RULE:[1:$0\$1](^GAUTO2QA\.GAUTO-QA\.COM\\.*)s/^GAUTO2QA\.GAUTO-QA\.COM/GAUTO2QA/
auth_to_local = RULE:[1:$0\$1](^GLOBEQE\.NET\\.*)s/^GLOBEQE\.NET/GLOBEQE/
auth_to_local = DEFAULT
kdc = examplehost.example.com
}
```

Note It is possible to have multiple kdc entries. However, it is not a requirement as in most cases there is only a single kdc value. If you choose to define additional kdc values, each line will have a kdc entry which will define a domain controller.

2 Restart the workspace service.

```
service horizon-workspace restart
```

See also Knowledge Base article 2091744.

Troubleshooting domain_krb.properties

Use the following information to troubleshoot the `domain_krb.properties` file.

"Error resolving domain" error

If the `domain_krb.properties` file already includes an entry for a domain, and you try to create a new directory of a different type for the same domain, an "Error resolving domain" occurs. You must edit the `domain_krb.properties` file and manually remove the domain entry before creating the new directory.

Domain controllers are unreachable

Once a domain entry is added to the `domain_krb.properties` file, it is not updated automatically. If any domain controllers listed in the file become unreachable, edit the file manually and remove them.

Managing User Attributes that Sync from Active Directory

During the VMware Identity Manager service directory setup, you select Active Directory user attributes and filters to select which users sync in the VMware Identity Manager directory. You can change the user attributes that sync from the administration console, Identity & Access Management tab, Setup > User Attributes.

Changes that are made and saved in the User Attributes page are added to the Mapped Attributes page in the VMware Identity Manager directory. The attributes changes are updated to the directory with the next sync to Active Directory.

The User Attributes page lists the default directory attributes that can be mapped to Active Directory attributes. You select the attributes that are required, and you can add other attributes that you want to sync to the directory. When you add attributes, the attribute name you enter is case-sensitive. For example, address, Address, and ADDRESS are different attributes.

Table 3-1. Default Active Directory Attributes to Sync to Directory

VMware Identity Manager Directory Attribute Name	Default Mapping to Active Directory Attribute
userPrincipalName	userPrincipalName
distinguishedName	distinguishedName
employeeId	employeeID
domain	canonicalName. Adds the fully qualified domain name of object.
disabled (external user disabled)	userAccountControl. Flagged with UF_Account_Disable When an account is disabled, users cannot log in to access their applications and resources. The resources that users were entitled to are not removed from the account so that when the flag is removed from the account users can log in and access their entitled resources
phone	telephoneNumber
lastName	sn
firstName	givenName

Table 3-1. Default Active Directory Attributes to Sync to Directory (Continued)

VMware Identity Manager Directory Attribute Name	Default Mapping to Active Directory Attribute
email	mail
userName	sAMAccountName.

The following attributes cannot be used as custom attribute names because VMware Identity Manager service uses these attributes internally for user identity management.

- externalUserDisabled
- employeeNumber

Select Attributes to Sync with Directory

When you set up the VMware Identity Manager directory to sync with Active Directory, you specify the user attributes that sync to the directory. Before you set up the directory, you can specify on the User Attributes page which default attributes are required and add additional attributes that you want to map to Active Directory attributes.

When you configure the User Attributes page before the directory is created, you can change default attributes from required to not required, mark attributes as required, and add custom attributes.

After the directory is created, you can change a required attribute not to be required, and you can delete custom attributes. You cannot change an attribute to be a required attribute.

Procedure

1. In the administration console, Identity & Access Management tab, click **User Attributes**.
2. In the Default Attributes section, review the required attribute list and make appropriate changes to reflect which attributes should be required.
3. Click **Save**.

Permissions Required for Joining a Domain (Linux Virtual Appliance Only)

You may need to join the VMware Identity Manager connector to a domain in some cases. For Active Directory over LDAP directories, you can join a domain after creating the directory. For directories of type Active Directory (Integrated Windows Authentication), the connector is joined to the domain automatically when you create the directory. In both scenarios, you are prompted for credentials.

To join a domain, you need Active Directory credentials that have the privilege to "join computer to AD domain". This is configured in Active Directory with the following rights:

- Create Computer Objects
- Delete Computer Objects

When you join a domain, a computer object is created in the default location in Active Directory, unless you specify a custom OU.

If you do not have the rights to join a domain, follow these steps to join the domain.

1 Ask your Active Directory administrator to create the computer object in Active Directory, in a location determined by your company policy. Provide the host name of the connector. Ensure that you provide the fully-qualified domain name, for example, `server.example.com`.

Tip You can see the host name in the **Host Name** column on the Connectors page in the administration console. Click **Identity & Access Management > Setup > Connectors** to view the Connectors page.

2 After the computer object is created, join the domain using any domain user account in the VMware Identity Manager administration console.

The **Join Domain** command is available on the **Connectors** page, accessed by clicking **Identity & Access Management > Setup > Connectors**.

Option	Description
Domain	Select or enter the Active Directory domain to join. Ensure that you enter the fully-qualified domain name. For example, **server.example.com**.
Domain User	The username of an Active Directory user who has the rights to join systems to the Active Directory domain.
Domain Password	The password of the user.
Organizational unit (OU)	(Optional) The organizational unit (OU) of the computer object. This option creates a computer object in the specified OU instead of the default Computers OU. For example, **ou=testou,dc=test,dc=example,dc=com**.

Important This topic applies only to the VMware Identity Manager service and connector Linux virtual appliances. It does not apply to the VMware Identity Manager service or connector on Windows.

Configuring Active Directory Connection to the Service

In the administration console, enter the information required to connect to your Active Directory and select users and groups to sync with the VMware Identity Manager directory.

The Active Directory connection options are Active Directory over LDAP or Active Directory (Integrated Windows Authentication). Active Directory over LDAP connection supports DNS Service Location lookup.

Prerequisites

- (SaaS) Connector installed and activated.
- Select which attributes are required and add additional attributes, on the User Attributes page. See Select Attributes to Sync with Directory.
- List of the Active Directory users and groups to sync from Active Directory.

- For Active Directory over LDAP, the information required includes the Base DN, Bind DN, and Bind DN password.

  Note Using a Bind DN user account with a non-expiring password is recommended.

- For Active Directory (Integrated Windows Authentication), the information required includes the domain's Bind user UPN address and password.

  Note Using a Bind DN user account with a non-expiring password is recommended.

- If the Active Directory requires access over SSL or STARTTLS, the Root CA certificate of the Active Directory domain controller is required.
- For Active Directory (Integrated Windows Authentication), when you have multi-forest Active Directory configured and the Domain Local group contains members from domains in different forests, make sure that the Bind user is added to the Administrators group of the domain in which the Domain Local group resides. If this is not done, these members are missing from the Domain Local group.

Procedure

1. In the administration console, click the **Identity & Access Management** tab.
2. On the Directories page, click **Add Directory**.
3. Enter a name for this VMware Identity Manager directory.

4 Select the type of Active Directory in your environment and configure the connection information.

Option	Description
Active Directory over LDAP	a In the **Sync Connector** text box, select the connector to use to sync with Active Directory. In an on premises deployment, a connector component is always available with the VMware Identity Manager service by default. This connector appears in the drop-down menu. If you install multiple VMware Identity Manager instances for high availability, the connector component of each appears in the list. Additional, external connectors are also listed. b In the **Authentication** text box, if this Active Directory is used to authenticate users, click **Yes**. If a third-party identity provider is used to authenticate users, click **No**. After you configure the Active Directory connection to sync users and groups, go to the Identity & Access Management > Manage > Identity Providers page to add the third-party identity provider for authentication. c In the **Directory Search Attribute** text box, select the account attribute that contains username. d If the Active Directory uses DNS Service Location lookup, make the following selections. ■ In the **Server Location** section, select the **This Directory supports DNS Service Location** check box. A `domain_krb.properties` file, auto-populated with a list of domain controllers, is created when the directory is created. See About Domain Controller Selection (domain_krb.properties file) . ■ If the Active Directory requires STARTTLS encryption, select the **This Directory requires all connections to use SSL** check box in the **Certificates** section and copy and paste the Active Directory Root CA certificate into the **SSL Certificate** text box. Ensure that the certificate is in the PEM format and includes the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. **Note** If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory. e If the Active Directory does not use DNS Service Location lookup, make the following selections. ■ In the **Server Location** section, verify that the **This Directory supports DNS Service Location** check box is not selected and enter the Active Directory server host name and port number. To configure the directory as a global catalog, see the Multi-Domain, Single Forest Active Directory Environment section in Active Directory Environments. ■ If the Active Directory requires access over SSL, select the **This Directory requires all connections to use SSL** check box in the **Certificates** section and copy and paste the Active Directory Root CA certificate into the **SSL Certificate** field.

Option	Description
	Ensure that the certificate is in the PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. **Note** If the Active Directory requires SSL and you do not provide the certificate, you cannot create the directory. f In the **Base DN** field, enter the DN from which to start account searches. For example, OU=myUnit,DC=myCorp,DC=com. g In the **Bind DN** field, enter the account that can search for users. For example, CN=binduser,OU=myUnit,DC=myCorp,DC=com. **Note** Using a Bind DN user account with a non-expiring password is recommended. h After you enter the Bind password, click **Test Connection** to verify that the directory can connect to your Active Directory.
Active Directory (Integrated Windows Authentication)	a In the **Sync Connector** text box, select the connector to use to sync with Active Directory. b In the **Authentication** text box, if this Active Directory is used to authenticate users, click **Yes**. If a third-party identity provider is used to authenticate users, click **No**. After you configure the Active Directory connection to sync users and groups, go to the Identity & Access Management > Manage > Identity Providers page to add the third-party identity provider for authentication. c In the **Directory Search Attribute** text box, select the account attribute that contains username. d If the Active Directory requires STARTTLS encryption, select the **This Directory requires all connections to use STARTTLS** check box in the **Certificates** section and copy and paste the Active Directory Root CA certificate into the **SSL Certificate** text box. Ensure that the certificate is in the PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines. If the directory has multiple domains, add the Root CA certificates for all domains, one at a time. **Note** If the Active Directory requires STARTTLS and you do not provide the certificate, you cannot create the directory. e (Linux only) Enter the name of the Active Directory domain to join. Enter a user name and password that has the rights to join the domain. See Permissions Required for Joining a Domain (Linux Virtual Appliance Only) for more information. f In the Bind User UPN text box, enter the User Principal Name of the user who can authenticate with the domain. For example, username@example.com. **Note** Using a Bind DN user account with a non-expiring password is recommended. g Enter the Bind User password.

5 Click **Save & Next**.

The page with the list of domains appears.

6 For Active Directory over LDAP, the domains are listed with a check mark.

For Active Directory (Integrated Windows Authentication), select the domains that should be associated with this Active Directory connection.

Note If you add a trusting domain after the directory is created, the service does not automatically detect the newly trusting domain. To enable the service to detect the domain, the connector must leave and then rejoin the domain. When the connector rejoins the domain, the trusting domain appears in the list.

Click **Next**.

7 Verify that the VMware Identity Manager directory attribute names are mapped to the correct Active Directory attributes and make changes, if necessary, then click **Next**.

8 Select the groups you want to sync from Active Directory to the VMware Identity Manager directory.

When groups are added here, group names are synced to the directory. Users that are members of the group are not synced to the directory until the group is entitled to an application or the group name is added to an access policy rule. Any subsequent scheduled syncs bring updated information from Active Directory for these group names.

Option	Description
Specify the group DNs	To select groups, you specify one or more group DNs and select the groups under them. a Click **+** and specify the group DN. For example, CN=users,DC=example,DC=company,DC=com. **Important** Specify group DNs that are under the Base DN that you entered. If a group DN is outside the Base DN, users from that DN will be synced but will not be able to log in. b Click **Find Groups**. The **Groups to Sync** column lists the number of groups found in the DN. c To select all the groups in the DN, click **Select All**, otherwise click **Select** and select the specific groups to sync. **Note** When you sync a group, any users that do not have Domain Users as their primary group in Active Directory are not synced.
Sync nested group members	The **Sync nested group members** option is enabled by default. When this option is enabled, all the users that belong directly to the group you select as well as all the users that belong to nested groups under it are synced when the group is entitled. Note that the nested groups are not synced; only the users that belong to the nested groups are synced. In the VMware Identity Manager directory, these users will be members of the parent group that you selected for sync. If the **Sync nested group members** option is disabled, when you specify a group to sync, all the users that belong directly to that group are synced. Users that belong to nested groups under it are not synced. Disabling this option is useful for large Active Directory configurations where traversing a group tree is resource and time intensive. If you disable this option, ensure that you select all the groups whose users you want to sync.

9 Click **Next**.

10 Specify the users to sync.

Because members in groups do not sync to the directory until the group is entitled to applications or added to an access policy rule, add all users who need to authenticate before group entitlements are configured.

a Click **+** and enter the user DNs. For example, CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com.

Important Specify user DNs that are under the Base DN that you entered. If a user DN is outside the Base DN, users from that DN will be synced but will not be able to log in.

b (Optional) To exclude users, create a filter to exclude some types of users.

You select the user attribute to filter by, the query rule, and the value.

11 Click **Next**.

12 Review the page to see how many users and groups are syncing to the directory and to view the sync schedule.

To make changes to users and groups, or to the sync frequency, click the **Edit** links.

13 Click **Sync Directory** to start the sync to the directory.

The connection to Active Directory is established and users and group names are synced from the Active Directory to the VMware Identity Manager directory. The Bind DN user has an administrator role in VMware Identity Manager by default.

What to do next

- If you created a directory that supports DNS Service Location, a `domain_krb.properties` file was created and auto-populated with a list of domain controllers. View the file to verify or edit the list of domain controllers. See About Domain Controller Selection (domain_krb.properties file).
- Set up authentication methods. After users and group names sync to the directory, if the connector is also used for authentication, you can set up additional authentication methods on the connector. If a third party is the authentication identity provider, configure that identity provider in the connector.
- Review the default access policy. The default access policy is configured to allow all appliances in all network ranges to access the Web portal, with a session time out set to eight hours or to access a client app with a session time out of 2160 hours (90 days). You can change the default access policy and when you add Web applications to the catalog, you can create new ones.
- (On premises) Apply custom branding to the administration console, user portal pages and the sign-in screen.

Enabling Users to Change Active Directory Passwords

You can provide users the ability to change their Active Directory passwords from the Workspace ONE portal or app whenever they want. Users can also reset their Active Directory passwords from the VMware Identity Manager login page if the password has expired or if the Active Directory administrator has reset the password, forcing the user to change the password at the next login.

You enable this option per directory, by selecting the **Allow Change Password** option in the Directory Settings page.

Users can change their passwords when they are logged into the Workspace ONE portal by clicking their name in the top-right corner, selecting **Account** from the drop-down menu, and clicking the **Change Password** link. In the Workspace ONE app, users can change their passwords by clicking the triple-bar menu icon and selecting **Password**.

Expired passwords or passwords reset by the administrator in Active Directory can be changed from the login page. When a user tries to log in with an expired password, the user is prompted to reset the password. The user must enter the old password as well as the new password.

The requirements for the new password are determined by the Active Directory password policy. The number of tries allowed also depends on the Active Directory password policy.

The following limitations apply.

- When a directory is added to VMware Identity Manager as a Global Catalog, the **Allow Change Password** option is not available. Directories can be added as Active Directory over LDAP or Integrated Windows Authentication, using ports 389 or 636.
- The password of a Bind DN user cannot be reset from VMware Identity Manager, even if it expires or the Active Directory administrator resets it.

  Note Using a Bind DN user account with a non-expiring password is recommended.

- Passwords of users whose login names consist of multibyte characters (non-ASCII characters) cannot be reset from VMware Identity Manager.

Note The Allow Change Password option cannot be enabled for ACC directories.

Prerequisites

- Port 464 must be open from VMware Identity Manager to the domain controllers. In a SaaS deployment, port 464 must be open from the VMware Identity Manager connector to the domain controllers.
- The **Allow Change Password** option is only available with connector version 2016.11.1 and later.

Procedure

1. In the administration console, click the **Identity & Access Management** tab.
2. In the **Directories** tab, click the directory.

3 In the **Allow Change Password** section, select the **Enable change password** checkbox.

4 Enter the Bind DN password in the **Bind User Details** section, and click **Save**.

Setting up Directory Sync Safeguards

Sync safeguards threshold limits can be configured in the directory to help prevent unintended configuration changes to the users and groups that sync to the directory from Active Directory.

The sync safeguard thresholds that are set limit the number of changes that can be made to the users and groups when the directory syncs. If any directory safeguard threshold is met, the directory synchronization stops and a message is displayed on the directory's Sync Log page. When SMTP is configured in the VMware Identity Manager administration console, you receive an email message when synchronization fails because of a safeguard violation.

When synchronization fails, you can go to the directory's Sync Settings > Sync Log page to see a description of the type of safeguard violation.

To successfully complete the synchronization, you can either increase the percentage threshold of the safeguard on the Sync Safeguard settings page, or you can schedule a dry run of the sync and check Ignore Safeguards. When you select to ignore the safeguard threshold value, the safeguard values are not enforced for this sync session only.

When directory sync is run the first time, the sync safeguard values are not enforced.

Note If you do not want to use the sync safeguards feature, delete the values from the drop-down menu. When the sync safeguard threshold text boxes are empty, sync safeguards are not enabled.

Configure Directory Sync Safeguards

Configure the sync safeguard threshold settings to limit the number of changes that can be made to the users and groups when the directory syncs.

Note If you do not want to use the sync safeguards feature, delete the values from the drop-down menu. When the sync safeguard threshold text boxes are empty, sync safeguards are not enabled.

Procedure

1 To change the safeguards settings, in the Identity & Access Management tab select **Manage > Directories**.

2 Select the directory to set the safeguards and click **Sync Settings**

3 Click **Safeguards**.

4 Set the percentage of changes to trigger the sync to fail.

5 Click **Save**.

Ignore Safeguard Settings to Complete Syncing to the Directory

When you receive notification that the sync did not complete because of a safeguard violation, to override the safeguard setting and complete the sync you can schedule a dry run of the sync and check Ignore Safeguards.

Procedure

1. In the Identity & Access Management tab select **Manage > Directories**.
2. Select the directory that did not complete the sync and go to the **Sync Log** page.
3. To see the type of safeguard violation, in the Sync Details column, click **Failed to complete sync. Please check safeguards**.
4. Click **OK**.
5. To continue the sync without changing the safeguard settings, click **Sync Now**.
6. On the Review page, select the check box **Ignore Safeguards**.
7. Click **Sync Directory**.

The directory sync is run and the safeguard threshold settings are ignored for this sync session only.

Integrating with LDAP Directories

4

You can integrate your enterprise LDAP directory with VMware Identity Manager to sync users and groups from the LDAP directory to the VMware Identity Manager service.

See also Chapter 2 Important Concepts Related to Directory Integration.

This section includes the following topics:

Limitations of LDAP Directory Integration

The following limitations currently apply to the LDAP directory integration feature.

- You can only integrate a single-domain LDAP directory environment.

  To integrate multiple domains from an LDAP directory, you need to create additional VMware Identity Manager directories, one for each domain.

- The following authentication methods are not supported for VMware Identity Manager directories of type LDAP directory.
  - Kerberos authentication
  - RSA Adaptive Authentication
  - ADFS as a third-party identity provider
  - SecurID
  - Radius authentication with Vasco and SMS Passcode server
- You cannot join an LDAP domain.
- Integration with Horizon or Citrix-published resources is not supported for VMware Identity Manager directories of type LDAP directory.
- User names must not contain spaces. If a user name contains a space, the user is synced but entitlements are not available to the user.

- If you plan to add both Active Directory and LDAP directories, ensure that you do not mark any attributes required in the User Attributes page, except for userName, which can be marked required. The settings in the User Attributes page apply to all directories in the service. If an attribute is marked required, users without that attribute are not synced to the VMware Identity Manager service.
- If you have multiple groups with the same name in your LDAP directory, you must specify unique names for them in the VMware Identity Manager service. You can specify the names when you select the groups to sync.
- The option to allow users to reset expired passwords is not available.
- The `domain_krb.properties` file is not supported.

Integrating an LDAP Directory with the Service

You can integrate your enterprise LDAP directory with VMware Identity Manager to sync users and groups from the LDAP directory to the VMware Identity Manager service.

To integrate your LDAP directory, you create a corresponding VMware Identity Manager directory and sync users and groups from the LDAP directory to the VMware Identity Manager directory. You can set up a regular sync schedule for subsequent updates.

You also select the LDAP attributes that you want to sync for users and map them to VMware Identity Manager attributes.

Your LDAP directory configuration might be based on default schemas or custom schemas. It may also have custom attributes. For VMware Identity Manager to be able to query your LDAP directory to obtain user or group objects, you need to provide the LDAP search filters and attribute names that are applicable to your LDAP directory.

Specifically, you need to provide the following information.

- LDAP search filters for obtaining groups, users, and the bind user
- LDAP attribute names for group membership, UUID, and distinguished name

Certain limitations apply to the LDAP directory integration feature. See Limitations of LDAP Directory Integration.

Prerequisites

- Review the attributes in the **Identity & Access Management > Setup > User Attributes** page and add additional attributes that you want to sync. You map the VMware Identity Manager attributes to your LDAP directory attributes when you create the directory. These attributes are synced for the users in the directory.

  Note When you make changes to user attributes, consider the effect on other directories in the service. If you plan to add both Active Directory and LDAP directories, ensure that you do not mark any attributes required except for **userName**, which can be marked required. The settings in the User Attributes page apply to all directories in the service. If an attribute is marked required, users without that attribute are not synced to the VMware Identity Manager service.

- A Bind DN user account. Using a Bind DN user account with a non-expiring password is recommended.
- In your LDAP directory, the UUID of users and groups must be in plain text format.
- In your LDAP directory, a domain attribute must exist for all users and groups.

  You map this attribute to the VMware Identity Manager **domain** attribute when you create the VMware Identity Manager directory.
- User names must not contain spaces. If a user name contains a space, the user is synced but entitlements are not available to the user.
- If you use certificate authentication, users must have values for userPrincipalName and email address attributes.

Procedure

1. In the administration console, click the **Identity & Access Management** tab.
2. In the Directories page, click **Add Directory** and select **Add LDAP Directory**.
3. Enter the required information in the Add LDAP Directory page.

Option	Description
Directory Name	A name for the VMware Identity Manager directory.
Directory Sync and Authentication	a In the **Sync Connector** text box, select the connector you want to use to sync users and groups from your LDAP directory to the VMware Identity Manager directory. In an on premises deployment, a connector component is always available with the VMware Identity Manager service by default. This connector appears in the drop-down list. If you install multiple VMware Identity Manager instances for high availability, the connector component of each appears in the list. Additional, external connectors are also listed. You do not need to use a separate connector for an LDAP directory. A connector can support multiple directories, regardless of whether they are Active Directory or LDAP directories. For the scenarios in which you need additional connectors, see *Installing and Configuring VMware Identity Manager*. b In the **Authentication** text box, if you want to use this LDAP directory to authenticate users, select **Yes**. If you want to use a third-party identity provider to authenticate users, select **No**. After you add the directory connection to sync users and groups, go to the **Identity & Access Management > Manage > Identity Providers page** to add the third-party identity provider for authentication. c In the **Directory Search Attribute** text box, specify the LDAP directory attribute to be used for user name. If the attribute is not listed, select **Custom** and type the attribute name. For example, **cn**.

Option	Description
Server Location	Enter the LDAP Directory server host and port number. For the server host, you can specify either the fully-qualified domain name or the IP address. For example, **`myLDAPserver.example.com`** or **`100.00.00.0`**. If you have a cluster of servers behind a load balancer, enter the load balancer information instead.
LDAP Configuration	Specify the LDAP search filters and attributes that VMware Identity Manager can use to query your LDAP directory. Default values are provided based on the core LDAP schema. **LDAP Queries** ■ **Get groups**: The search filter for obtaining group objects. For example: **`(objectClass=group)`** ■ **Get bind user**: The search filter for obtaining the bind user object, that is, the user that can bind to the directory. For example: **`(objectClass=person)`** ■ **Get user**: The search filter for obtaining users to sync. For example:**`(&(objectClass=user)(objectCategory=person))`** **Attributes** ■ **Membership**: The attribute that is used in your LDAP directory to define the members of a group. For example: **`member`** ■ **Object UUID**: The attribute that is used in your LDAP directory to define the UUID of a user or group. For example: **`entryUUID`** ■ **Distinguished Name**: The attribute that is used in your LDAP directory for the distinguished name of a user or group. For example: **`entryDN`**
Certificates	If your LDAP directory requires access over SSL, select the **This Directory requires all connections to use SSL** and copy and paste the LDAP directory server's root CA SSL certificate. Ensure the certificate is in PEM format and include the "BEGIN CERTIFICATE" and "END CERTIFICATE" lines.
Bind User Details	**Base DN**: Enter the DN from which to start searches. For example, cn=users,dc=example,dc=com **Bind DN**: Enter the user name to use to bind to the LDAP directory. **Note** Using a Bind DN user account with a non-expiring password is recommended. **Bind DN Password**: Enter the password for the Bind DN user.

4 To test the connection to the LDAP directory server, click **Test Connection**.

If the connection is not successful, check the information you entered and make the appropriate changes.

5 Click **Save & Next**.

6 In the Domains page, verify that the correct domain is listed, then click **Next**.

7 In the Map Attributes page, verify that the VMware Identity Manager attributes are mapped to the correct LDAP attributes.

These attributes will be synced for users.

Important You must specify a mapping for the **domain** attribute.

You can add attributes to the list from the User Attributes page.

8 Click **Next**.

9 In the groups page, click **+** to select the groups you want to sync from the LDAP directory to the VMware Identity Manager directory.

When groups are added, group names are synced to the directory. Users that are members of the group are not synced to the directory until the group is entitled to an application or the group name is added to an access policy rule.

If you have multiple groups with the same name in your LDAP directory, you must specify unique names for them in the groups page.

The **Sync nested group users** option is enabled by default. When this option is enabled, all the users that belong directly to the group you select as well as all the users that belong to nested groups under it are synced. Note that the nested groups are not synced; only the users that belong to the nested groups are synced when the group is entitled. In the VMware Identity Manager directory, these users will appear as members of the top-level group that you selected for sync. In effect, the hierarchy under a selected group is flattened and users from all levels appear in VMware Identity Manager as members of the selected group.

If this option is disabled, when you specify a group to sync, all the users that belong directly to that group are synced. Users that belong to nested groups under it are not synced. Disabling this option is useful for large directory configurations where traversing a group tree is resource and time intensive. If you disable this option, ensure that you select all the groups whose users you want to sync.

10 Click **Next**.

11 Click **+** to add users. For example, enter **`CN=username,CN=Users,OU=myUnit,DC=myCorp,DC=com`**.

Because members in groups do not sync to the directory until the group is entitled to applications or added to an access policy rule, add all users who need to authenticate before group entitlements are configured.

To exclude users, create a filter to exclude some types of users. You select the user attribute to filter by, the query rule, and the value.

Click **Next**.

12 Review the page to see how many users and group names will sync to the directory and to view the default sync schedule.

To make changes to users and groups, or to the sync frequency, click the **Edit** links.

13 Click **Sync Directory** to start the directory sync.

The connection to the LDAP directory is established and users and group names are synced from the LDAP directory to the VMware Identity Manager directory. The Bind DN user has an administrator role in VMware Identity Manager by default.

Adding a Directory After Configuring Failover and Redundancy

5

If you add a new directory to the VMware Identity Manager service after you have already deployed a cluster for high availability, and you want to make the new directory part of the high availability configuration, you need to add the directory to all the instances in your cluster.

In an on-premises deployment, you do this by adding the connector component of each of the service instances to the new directory. In a SaaS deployment, you do this by adding all the connector instances to the new directory.

Procedure

1. Log in to the VMware Identity Manager administration console.
2. Select the **Identity & Access Management** tab, then select the **Identity Providers** tab.
3. In the Identity Providers page, find the identity provider for the new directory and click the identity provider name.
4. In the **IdP Hostname** field, enter the load balancer FQDN, if it is not already set to the correct load balancer FQDN.

   Note This step is required only if you are using a load balancer. In a SaaS deployment, using a load balancer in front of connectors in outbound-only connection mode is not a requirement. However, if you have set up a load balancer for certain scenarios such as Kerberos authentication, enter the load balancer FQDN here.

5. In the **Connector(s)** field, select the connector to add.
6. Enter the password and click **Save**.
7. In the Identity Providers page, click the Identity Provider name again and verify that the **IdP Hostname** field displays the load balancer FQDN. If the name is incorrect, enter the load balancer FQDN and click **Save**.
8. Repeat the previous steps to add all the connectors listed in the **Connector(s)** field.

   Note After you add each connector, check the IdP host name and modify it, if necessary, as described in step 7.

   The directory is now associated with all the connectors in your deployment.