VMware NSX Network Detection and Response LDAP Integration

Contents

VMware NSX Network Detection and Response LDAP Integration

Integration with an external LDAP server provides authentication and authorization services for the User Portal running on On-Premises appliances.

About LDAP Integration

To provide additional authentication and authorization security services, VMware supports the integration of the Analyst, Manager and/or All-In-One with an external LDAP server.

Requirements

The following are required for LDAP integration:

- VMware NSX Network Detection and Response On-Premises 9.0 or higher
- An LDAPv3-compatible server (this has been tested with Microsoft Active Directory on Windows Server 2016)
- Group entries in the directory must have a multi-valued attribute which contains the FDN of the user entry of each user in the group (the `member` attribute supplied by Active Directory satisfies this requirement)
- Either all user and group entries must be readable via anonymous bind or an integration user must be configured with sufficient access to read all user and group entries (for Active Directory with default integration options, this means the integration user needs a minimum of read permission for the `userPrincipalName` attribute of user entries and the `member` attribute of group entries). It is recommended that you create an integration user with read-only access to the LDAP server, as the credentials for the integration user are stored on the VMware appliance.
- In order to use LDAPS, the certificate for each LDAP server must be signed by a CA trusted by the VMware appliance (the CA listed in `/etc/ssl/certs/ca-certificates.crt`). It is possible to use LDAP without SSL, however this is strongly discouraged, as the LDAP bind operation is vulnerable to network snooping.

LDAP Configuration

Configuration Steps

Use the `lastline_configure_ldap_integration.py` script to configure LDAP integration on the Analyst, Manager and/or All-In-One appliance. This script is part of the NSX PAPI client implementation, the *papi-client* (https://user.lastline.com/papi-doc/api/html/api/client.html). The script requires:

- python 3.8
- *requests* (https://requests.readthedocs.io/en/latest/) module (version 3 or above)

Basic usage of the `lastline_configure_ldap_integration.py` script is:

```
lastline_configure_ldap_integration.py [option ...] subcommand [...]
```

The script accepts the following command line options:

Command Line	Purpose
`-c`	Use the defined configuration file.
`--name`	The name of the directory configuration.
`--server`	The server for the directory configuration. Specified as *`hostname`*`[:`*`port`*`]`. The default port is 636 for LDAPS or 389 for LDAP. The server can be specified multiple times.
`--no_ssl`	Use LDAP rather than LDAPS when connecting to the directory servers. This is strongly discouraged, as the LDAP bind operation is vulnerable to network snooping.
`--user-search-base`	FDN of the directory entry under which to search for users, for example `DC=example,DC=com`.
`--user-search-filter`	Filter expression used to search for users, with `{}` in place of username.
`--strategy`	Provisioning strategy for assigning users to groups.
`--integration-user`	User to bind to read users/groups. For Active Directory, the integration user must be in the format *`username`*`@`*`domain`* (UPN format). **Note:** This field has a limit of 64 characters.
`--integration-password`	Password for user to bind to read users/groups.

Command Line	Purpose
`--group-search-base`	FDN of the directory entry under which to search for groups. For example `DC=example,DC=com`.
`--group-search-filter`	Filter expression used to search for groups, with `{}` in place of FDN of user in group.
`--group-name-attribute`	Attribute of the group entry which stores the group's name.

The script supports the following sub-commands:

Sub-Command	Purpose
`list`	List basic information about all LDAP directory configurations.
`info` *uuid*	List detailed information about the specified LDAP directory configuration.
`add [...]`	Add an LDAP directory configuration.
`update` *uuid* `[...]`	Update the specified LDAP directory configuration.
`add-group` *uuid group role*	Add a mapping from the specified LDAP group to an account role.
`delete-group` *uuid group*	Delete the mapping from the specified LDAP group to an account role.

Procedure

Step 1: Download and install the papi-client

Download the NSX PAPI software from the *User Portal* (https://user.lastline.com/papi-doc/api/client/papi_client.tar.gz). Decompress the `papi_client.tar.gz` file and install it.

Step 2: Create a configuration file

Create a configuration file structured similar to the following:

```
[papi]
url = https://user.lastline.com/papi
auth_method = account
username = user@example.com
password = portal_password
verify_ssl = true|false
timeout = seconds
```

Name the configuration file, for example, `config.ini`. The `[papi]` section is required and consists of the following entries:

- `url` — URL to reach the VMware backend. For NSX PAPI, use `https://user.lastline.com/papi`.

- auth_method — Method of authentication. Must be "account".
- username — User Portal account username.
- password — User Portal account password.
- verify_ssl — Defines whether to perform SSL certificate validation. Set this to "false" if you are using a self-signed certificate.
- timeout — HTTP request timeout in seconds. "20" is recommended.

Step 3: Add a new configuration

Use the add sub-command of the lastline_configure_ldap_integration.py script to add a new directory configuration for an Active Directory server, example.com:

```
lastline@lastline-manager:~$ lastline_configure_ldap_integration.py -c config.ini add \
--name "Example Directory" --server example.com --user-search-base DC=example,DC=com \
--integration-user readonly@example.com --integration-password password
```

The add sub-command returns the UUID of the LDAP directory configuration which is used in the following step.

Step 4: Add user groups to the configuration

Populate the map from LDAP groups to VMware account roles through multiple uses of the add-group sub-command:

```
lastline@lastline-manager:~$ lastline_configure_ldap_integration.py -c config.ini add-group \
d41d8cd98f00b204e9800998ecf8427e Reviewers read_only
lastline@lastline-manager:~$ lastline_configure_ldap_integration.py -c config.ini add-group \
d41d8cd98f00b204e9800998ecf8427e Analysts analyst
```

In the above example:

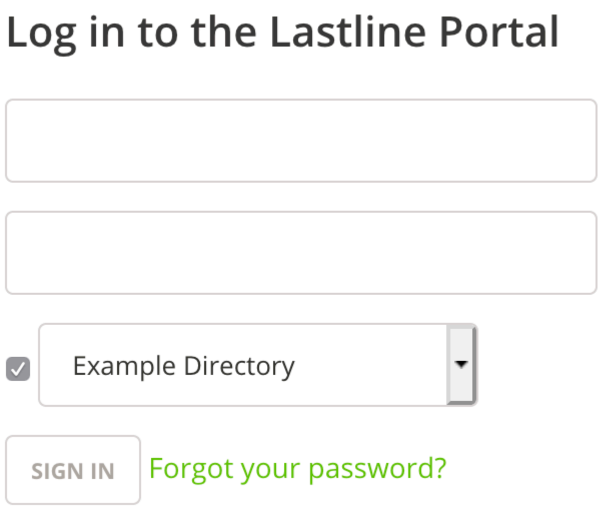
- The values of d41d8cd98f00b204e9800998ecf8427e and d41d8cd98f00b204e9800998ecf8427e refer to the UUID that was returned in the previous step.
- The values of Reviewers and Analysts refer to the LDAP group name.
- The values of read_only and analyst refer to the VMware NSX Network Detection and Response role.

Note: If the group name attribute is not configured (--group-name-attribute ""), LDAP groups are specified by FDN rather than by name in the group-to-role map.

LDAP Login

Configuration Steps

Once the configuration of LDAP integration is complete, the option to use LDAP for login to the User Portal is displayed:



Log in to the Lastline Portal

LDAP Sign On ☑ Example Directory

To login using LDAP:

Procedure

Step 1: Enable LDAP sign on

Select the LDAP Sign On by clicking the **[☑]** (it is selected by default).

Step 2: Select the appropriate LDAP directory

Select the appropriate LDAP directory from the drop-down menu. The directories are listed in alphabetical order. The first directory is selected by default.

Step 3: Enter your LDAP credentials

Use the Username and Password fields to enter your LDAP credentials. Click **[SIGN IN]** to login to the User Portal.

Note: Your account must belong to at least one group which is mapped to a role before you will be allowed to log into the User Portal.

For Active Directory, your Username must be in the format `username@domain` (UPN format).

LDAP Administration

When your users login to the User Portal via LDAP integration, they are granted the roles associated with their LDAP groups on a temporary basis. Such roles will persist until the next time the user logs in. Changes to an LDAP user's groups will be reflected the next time they log in.

When an LDAP user logs into the User Portal for the first time, a VMware NSX Network Detection and Response account is created automatically, if it does not already exist. Accounts created in this manner have no password and no permanent permissions. An administrator can grant roles and permissions (including the permission to set a password) to this account like any other account.

If an LDAP user is removed from all the groups in the configured group-to-role map (or if the group-to-role map is changed to no longer include any of the user's groups), that user will no longer be able to log into the User Portal via LDAP. Be aware that, if the user was granted permission to set a password and has done so, they will still be able to login to the portal using that password. To prevent portal access in this case, you must block the user using the All accounts tab of the User Portal.

Release History

Release	Date	Description
On-Premises 9.0	2019-Oct-24	Initial release of LDAP integration

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