Designlet: Identity and Access Management for Azure VMware Solution

VMware Getting Started

Table of contents

Designlet: Identity and Access Management for Azure VMware Solution

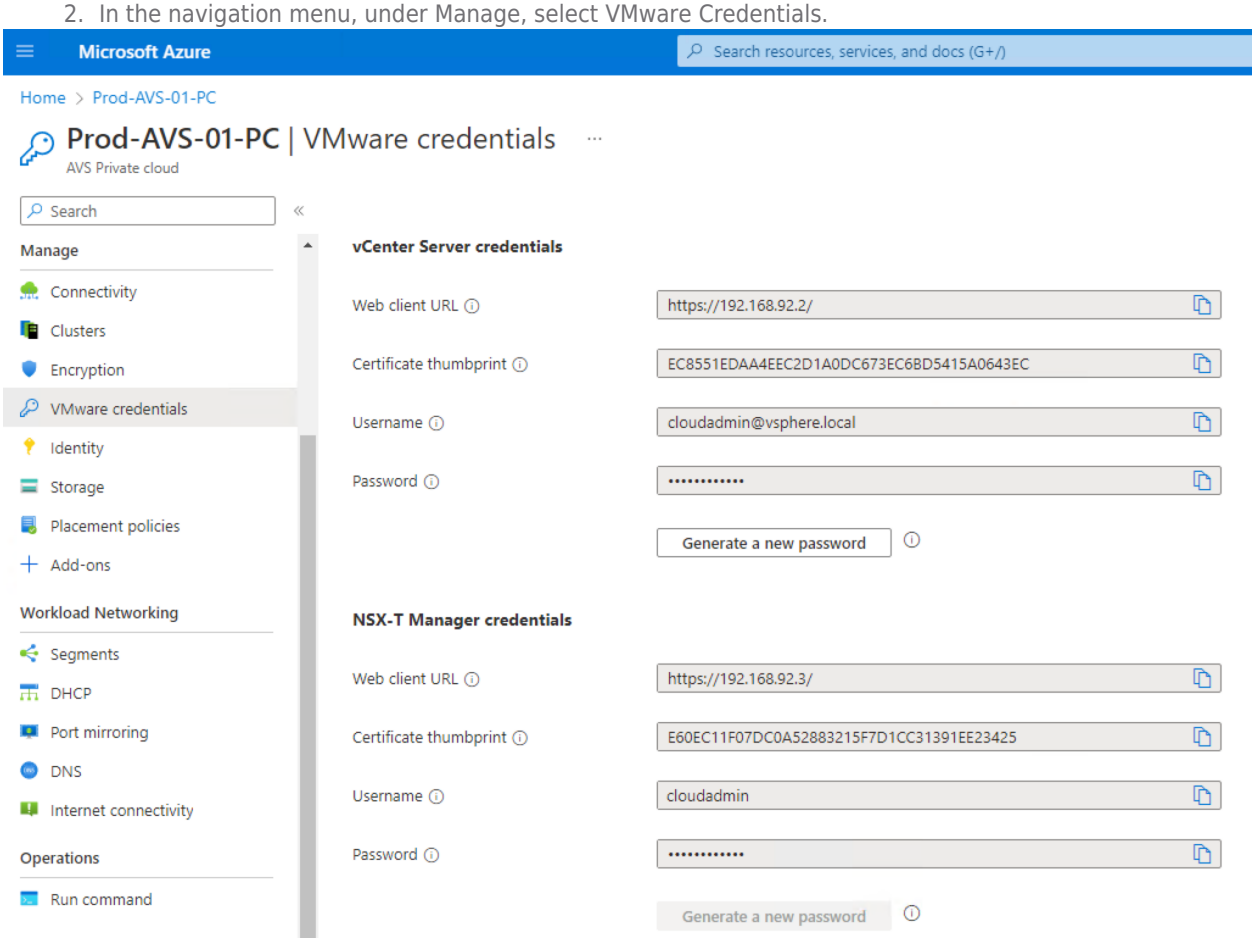
Introduction

Azure VMware Solution (AVS) private clouds are provisioned with VMware vCenter Server and NSX-T. They leverage vSphere role-based access control (RBAC) for management, flexibility, and enhanced security. After deployment customers can access both vCenter and NSX-T Manager using the local, built-in, **cloudadmin** user account, which is assigned to the **cloudadmin** role with a specific set of permissions.

Private clouds created before June 2022 will utilize the local, built-in, **admin** user account to access NSX-T manager. This will be changed over to **cloudadmin** at somepoint in the future, and customers will receive a notification through Azure Service Health with more details.

To access the credentials:

1. Login to the Azure portal and search for your AVS private cloud.
2. In the navigation menu, under Manage, select VMware Credentials.



Administrative access, or root, for ESXi hosts is restricted.

Summary and Considerations

Use Case	Identity and access management for vCenter Server and NSX-T in an Azure VMware Solution private cloud.
Pre-requisites	**For configuring an external identity source:** **For changing vCenter or NSX-T `cloudadmin` passwords:**
General Considerations/Recommendations	The `cloudadmin` account should be used for emergency access only. It should not be used for regular administrative access or integration with other services. The `vsphere.local` SSO domain is a managed resource; it does not support the creation and management of local users and groups.
Performance Considerations	If configuring an external identity source, consider deploying a domain controller inside of the AVS private cloud to avoid sending authentication and DNS traffic across the WAN.
Cost Implications	Egress charges may apply to traffic communicating from Azure VMware Solution to an on-premises environment.
Document Reference	VMware documentation for defined privileges Best Practices for vCenter Roles and Permissions Delegate access with shared assess signatures (SAS)
Last Updated	January 2023

VMware vCenter Server

By default, the vCenter Server uses a local account `cloudadmin@vsphere.local`, which is assigned to the CloudAdmin role. As an administrator of the AVS private cloud, you have access to this account. However, while it has near-admin privileges, it is not the same as it's on-premises counterpart `administrator@vsphere.local`.

Administrators of the private cloud do not have access to the `administrator@vsphere.local` account, and because of this, cannot manage specific components of the vSphere environment such as adding identity sources via traditional methods, or managing clusters, hosts, datastores, and distributed virtual switches.

CloudAdmin Role

The CloudAdmin role allows you to manage most aspects of the private cloud, except the components that Microsoft supports and manages as part of the service. The CloudAdmin role has the following privileges:

Privilege	Description
Alarms	Acknowledge alarm Create alarm Disable alarm action Modify alarm Remove alarm Set alarm status
Content Library	Add library item Add root certificate to trust store Check in a template Check out a template Create a subscription for a published library Create local library Create or delete a Harbor registry Create subscribed library Delete a Harbor image or Harbor registry project Delete library item Delete local library Delete root certificate from trust store Delete subscribed library Delete subscription of a published library Evict library item Evict library items Evict subscribed library Import storage Manage Harbor registry resource on specified compute resource Probe subscription information Publish a library item to its subscribers Publish a library to its subscribers Sync library item Sync library items Sync subscribed library Type introspection Update configuration settings Update files Update library Update library item Update local library Update subscribed library Update subscription of a published library View configuration settings
Cryptographic operations	Direct access
Datastore	Allocate space Browse datastore Configure datastore Low level file operations Remove file Update virtual machine metadata
Folder	Create folder Delete folder Move folder Rename folder
Global	Cancel task Global tag Health Log event Manage custom attributes Set custom attribute Set custom attribute System tag
Host	vSphere Replication Manage replication
Network	Assign network
Permissions	Modify permissions Modify role
Profile	Profile-driven storage view
Resource	Apply recommendation Assign vApp to resource pool Assign virtual machine to resource pool Create resource pool Migrate powered off virtual machine Migrate powered on virtual machine Modify resource pool Query vMotion Query vMotion Remove resource pool Rename resource pool
Scheduled task	Create task Modify task Remove task Run task
Sessions	Message Validate session
Storage view	View
vApp	Add virtual machine Assign resource pool Assign vApp Clone Create Delete Export Import Move Power off Power on Rename Suspend Unregister View OVF environment vApp application configuration vApp instance configuration vApp managedBy configuration vApp resource configuration
Virtual machine	Change Configuration Acquire disk lease Add existing disk Add new disk Add or remove device Advanced configuration Change CPU count Change memory Change Settings Change swapfile placement Change resource Configure host USB device Configure raw device Configure managedBy Display connection settings Extend virtual disk Modify device settings Query Fault Tolerance compatibility Query unowned files Reload from path Remove disk Rename Reset guest information Set annotation Toggle disk change tracking Toggle fork parent Upgrade virtual machine compatibility Add inventory Create from existing Create new Move Register Remove Unregister Guest operations Guest operation alias modification Guest operation alias query Guest operation modifications Guest operation program execution Guest operation queries Interaction Answer question Back up operation on virtual machine Configure CD media Configure floppy media Connect devices Console interaction Create screenshot Defragment all disks Drag and drop Guest operating system management by VIX API Inject USB HID scan codes Install VMware Tools Pause or unpause Wipe or shrink operations Power off Power on Record session on virtual machine Replay session on virtual machine Reset Resume Fault Tolerance Suspend Suspend fault tolerance Take snapshot Test restart secondary VM Turn off fault tolerance Turn on fault tolerance Provisioning Allow disk access Allow file access Allow read-only disk access Allow virtual machine download Allow virtual machine files upload Clone virtual machine Create template from virtual machine Customize guest Deploy template Mark as template Modify customization specification Promote disks Read customization specifications Service configuration Allow notifications Allow polling of global event notifications Manage service configurations Modify service configuration Query service configurations Read service configuration Snapshot management Create snapshot Remove snapshot Rename snapshot Revert snapshot vSphere Replication Configure replication Monitor replication Monitor replication
vService	Create dependency Destroy dependency Reconfigure dependency configuration Update dependency
vSphere tagging	Assign and unassign vSphere tag Create vSphere tag Create vSphere tag category Delete vSphere tag Delete vSphere tag category Edit vSphere tag Edit vSphere tag category Modify Usedby field for category Modify Usedby field for tag

Custom Roles

AVS supports custom roles with equal or lesser privileges to the CloudAdmin role.

Note: If you create roles with privileges greater that the CloudAdmin role, you won't be able to assign or delete the role.

Creating Custom Roles

3. Login to vCenter with `cloudadmin@vsphere.local` or a user account with the CloudAdmin role.
4. Select **Menu** > **Administration**
5. Under **Access Control**, select **Roles**
6. Select the **CloudAdmin** role, and then the **Clone role action icon**
7. Provide a name for the new role.
8. Modify the privileges for the role and select **OK**.

Applying Custom Roles

Custom roles are applied to specific objects and can be propagated down from the parent. In this example, we'll apply a custom role to a virtual machine folder object.

Note: Since local users and groups cannot be created in the `vsphere.local` SSO domain, you must have an external identity source configured to apply a custom role to a particular Active Directory user or group.

1. Select **Menu** > **VMs and Templates**
2. Right-click on the folder where you want to add the role and then **Add Permission**
3. Select the Identity Source in the User drop-down

4. Search for the user or group you want to add
5. Select the role you want to apply to the user or group
6. If necessary, check **Propagate to children**, and select **OK**

Change cloudadmin password

A complex password is automatically generated during the provisioning of your private cloud for `cloudadmin@vsphere.local`.

The password for this account does not expire, but you can change it at any time via the Azure Portal within the **VMware credentials** blade, or using the Azure Cloud Shell. Simply open a new session and execute the following command.

Note: Replace {SubscriptionID}, {ResourceGroup}, and {PrivateCloudName] with your information.

```
az resource invoke-action --action rotateVcenterPassword --ids
"/subscriptions/{SubscriptionID}/resourceGroups/{ResourceGroup}/providers/Microsoft.AVS/privateClouds/{PrivateCloudNam
e}" --api-version "2020-07-17-preview"
```

Consider and stop all services and third-party tools that connect or integrate via these accounts prior to changing the password(s). Services and tools may include, but are not limited to:

- VMware HCX
- VMware Site Recovery Manager
- VMware Horizon
- vRealize suite of products
- Backup services
- Monitoring services

These services will stop working and may cause the account to become locked after multiple authentication attempts if they continue to use the previous password.

Services that leverage site pairs between multiple vCenter Servers such as VMware HCX and VMware Site Recovery Manager will require the site pair to be modified with the new password and re-established.

External Identity Source

The CloudAdmin role in vCenter Server allows administrators to assign Active Directory users and groups to the CloudAdmin role, or other custom roles. However, it does not have permission to add an LDAP or LDAPS identity source via traditional methods. Instead, the Azure Run command feature allows you to perform tasks that would normally require elevated privileges through a collection of PowerShell cmdlets such as:

- Listing existing identity sources currently integrated with vCenter Server
- Adding or removing Active Directory over LDAP identity sources, with or without SSL
- Adding or removing existing Active Directory groups to the CloudAdmin role

Run commands can be accessed from within your **Azure VMware Solution private cloud** in the **Azure portal** under **Operations** > **Run command**. Afterwards, check **Notifications** or the **Run Execution Status** pane to see the progress and output.

List External Identity Sources

1. In the Run command pane, select **Packages** > **Get-ExternalIdentitySources**
2. Fill in the **required fields** and select **Run**

Required Field	Description
Retain up to	Retention period of the cmdlet output. The default value is 60 days.
Specify name for execution	Alphanumeric name. Example: **getIdentitySources.**
Timeout	The period after which a cmdlet exits if taking too long to finish.

Add Active Directory over LDAP

It is best practice to use Active Directory over LDAP with SSL, outlined in the next section, over this method.

3. In the Run command pane, select **Packages** > **New-AvsLDAPIdentitySource**
4. Fill in the **required fields** and select **Run**

Required Field	Description
Name	Friendly name of the identity source. Example: **stickers.corp.**
DomainName	FQDN of the domain.
DomainAlias	For Active Directory identity sources, the domain's NetBIOS name. Add the NetBIOS name of the AD domain as an alias of the identity source if you're using SSPI authentications.
PrimaryUrl	Primary URL of the external identity source. Example: **ldap://nyc-dc-01.stickers.corp:389**
SecondaryUrl	Fall-back URL if there is a primary failure.
BaseDNUsers	The Base DN used to search for users. Example: **CN=users,DC=stickers,DC=corp**
BaseDNGroups	The Base DN used to search for groups. Example: **CN=groups,DC=stickers,DC=corp**
Credential	Credentials used for Active Directory authentication.
GroupName	Active Directory group that should be granted access to the CloudAdmin role.
Retain up to	Retention period of the cmdlet output. The default value is 60 days.
Specify name for execution	Alphanumeric name. Example: **addIdentitySource.**
Timeout	The period after which a cmdlet exits if taking too long to finish.

Add Active Directory over LDAP with SSL

Active Directory over LDAP with SSL is the preferred method for authentication.

Prior to configuring the identity source, you must upload the certificate(s) from your domain controller(s) for AD authentication to an Azure Storage account as blob storage. Access to the Azure storage resource will need to be granted using a shared access signature (SAS). The SAS strings for each certificate are supplied to the cmdlet as a parameter.

Note: Be sure to copy each SAS string, and store it in a secure location, when it's created as they are no longer available when you leave the page.

The required fields are the save as above, with one addition.

1. In the Run command pane, select **Packages** > **New-AvsLDAPSIdentitySource**
2. Fill in the **required fields** and select **Run**

Required Field	Description
CertificateSAS	Path to SAS strings with the certificates for authentication to the AD source. If you're using multiple certificates, separate each SAS string with a comma. Example: pathtocert1,pathtocert2.

Add/Remove Active Directory Group to/from the CloudAdmin Role

These cmdlets will allow you to add an existing Active Directory group to the CloudAdmin Role, which will provide the users within the group privileges equal to `cloudadmin@vsphere.local`. You can also remove Active Directory groups from this role.

To add a group:

1. In the Run command pane, select **Packages** > **Add-GroupToCloudAdmins**
2. Fill in the **required fields** and select **Run**

To remove a group:

1. In the Run command pane, select **Packages** > **Remove-GroupFromCloudAdmins**
2. Fill in the **required fields** and select **Run**

Required Field	Description
GroupName	Name of the Active Directory group to add or remove. Example: **AVSAdmins**
Retain up to	Retention period of the cmdlet output. The default value is 60 days.
Specify name for execution	Alphanumeric name. Example: **addADGroup, removeADGroup.**
Timeout	The period after which a cmdlet exits if taking too long to finish.

Remove Identity Sources

This cmdlet removes all existing external identity sources, in bulk. Use with caution.

1. In the Run command pane, select **Packages** > **Remove-ExternalIdentitySources**
2. Fill in the **required fields** and select **Run**

Required Field	Description
Retain up to	Retention period of the cmdlet output. The default value is 60 days.
Specify name for execution	Alphanumeric name. Example: **removeIdentitySources.**
Timeout	The period after which a cmdlet exits if taking too long to finish.

VMware NSX-T

Microsoft is responsible for the initial NSX-T configuration, including the Tier-0 (T0) gateway, as well as life cycle management.

Customers are responsible for the remainder of the configuration, including:

- Tier-1 (T1) gateways
- Network segments (logical switches)
- Distributed firewall rules
- Gateway firewall rules
- Load balancers on T1 gateways
- Other stateful services

Some operations are not permitted by customers such as T0, host, and edge transport node configurations.

Admin Role

Private clouds created before June 2022 will utilize the local, built-in, **admin** user account to access NSX-T manager. This will be changed over to **cloudadmin** at somepoint in the future, and customers will receive a notification through Azure Service Health with more details.

Private clouds created after June 2002 will utilize the local, built-in, **cloudadmin** user account.

CloudAdmin Role

The CloudAdmin role for NSX-T manager is different than the one used for vCenter Server. The CloudAdmin role has the following privileges:

Category	Type	Operation	Permission
Networking	Connectivity	Tier-0 Gateways Tier-1 Gateways Segments	Read-only Full Access Full Access
Networking	Network Services	VPN NAT Load Balancing Forwarding Policy Statistics	Full Access Full Access Full Access Read-only Full Access
Networking	IP Management	DNS DHCP IP Address Pools	Full Access
Networking	Profiles		Full Access
Security	East West Security	Distributed Firewall Distributed IDS and IPS Identity Firewall	Full Access
Security	North South Security	Gateway Firewall URL Analysis	Full Access
Security	Settings		Full Access
Security	Network Introspection		Read-only
Security	Endpoint Protection		Read-only
Inventory			Full Access
Troublshooting	IPFIX Port Mirroring Traceflow		Full Access
System	Configuration Settings	Identity Firewall Users and Roles Cert Management (Service Cert only) User Interface Settings	Full Access
System	All other		Read-only

External Identity Source

RBAC using external identity sources can be leveraged to manage access to NSX-T manager.

List External Identity Sources

1. Login to NSX-T Manager using the admin account.
2. Navigate to **System** > **Users and Roles** > **LDAP**

The table will list all configured identity sources.

Add External Identity Source

Active Directory over LDAP with SSL is the preferred method for authentication.

1. Click the **Add Identity Source** button
2. Fill in the **required fields**

Required Field	Description
Name	Friendly name of the identity source. Example: **stickers.corp.**
Domain Name (FQDN)	FQDN of the domain.
Base DN	The Base DN used to search for users. Example: **CN=users,DC=stickers,DC=corp**
Type	Active Directory over LDAP

3. Under **LDAP Servers**, click **Set**
4. Click the **Add LDAP Server** button
5. Fill in the **required fields**
6. Leave the **Certificate** field blank, even if using LDAPS.

Required Field	Description
Hostname/IP	Primary URL of the external identity source. Example: **avs-dc-01.stickers.corp**
LDAP Protocol	LDAP or LDAPS
Port	389 or 636 (will update automatically based on protocol chosen).
Bind Identity	Username used for Active Directory authentication.
Password	Password of the Bind Idendity used for Active Directory authentication.

7. Under Connection Status, click Check Status
8. If prompted, **accept** the certificate for your LDAP server
9. Click the **Add** button, then **Apply**, then **Save**
10. Under **Connection Status**, click **Check Status** once more to verify the connection is successful.

Remove External Identity Source

1. Login to NSX-T Manager using the admin account.
2. Navigate to **System** > **Users and Roles** > **LDAP**

The table will list all configured identity sources.

3. Select the **Available Actions Menu** (3 dots) next to the identity source you with to remove, then **Delete**
4. When prompted for verification, click **DELETE**

Custom Roles

Adding Active Directory users and groups directly to existing NSX roles is supported, however it is recommended to clone existing roles or create custom roles for these users and groups. AVS supports custom roles with equal or lesser privileges to the cloudadmin role.

Supported and Unsupported Roles

The following predefined roles are supported with LDAP integration:

- Auditor
- Cloudadmin
- LB Admin
- LB Operator
- VPN Admin
- Network Operator

The following predefined roles are not supported with LDAP integration:

- Enterprise Admin
- Network Admin
- Security Admin
- Netx Partner Admin
- GI Partner Admin

Creating Custom Roles

1. Login to NSX-T Manager using the admin account.
2. Navigate to **System** > **Users and Roles** > **Roles**

You have the option to add a new custom role by clicking the **Add Role** button, or cloning an existing role. In this example we will clone the **Network Admin** role.

3. Select the Available Actions Menu (3 dots) next to Network Admin, then Clone
4. Provide a name for the new role
5. Modify the privileges for the role if necessary, then click **Save**

Applying Custom Roles

1. Still logged in to NSX-T Manager, Navigate to **System** > **Users and Roles** > **User Role Assignment**
2. Select **Add** > **Role Assignment for LDAP**
3. Under **Search Domain**, select your Active Directory domain.
4. Under **Search User/User Group**, type the name of the user or group you wish to assign the role.
5. Select the custom role you created from the **Roles** drop down.
6. Click **Save.**

Users will now be able to login to NSX-T manager with their Active Directory credentials to perform tasks allowed based on their role assignment.

Change admin password

At the time of this writing, changing the NSX-T Manager `admin` password is not supported. If a password change is necessary, please open a support request via the Azure portal. Changing this password may impact HCX services and require re-authentication.

Authors and Contributors

- Jeremiah Megie, Principal Cloud Solutions Architect, CIBG, VMware
- Steve Pantol, Senior Technical Marketing Architect, CIBG, VMware

Changelog

The following updates were made to this guide:

Date	Description of Changes
2023/01/13	
2021/12/06	
2021/10/05