Set-LapsADReadPasswordPermission

https://learn.microsoft.com/en-us/powershell/module/laps/set-lapsadreadpasswordpermission?view=windowsserver2022-ps

Syntax

PowerShell Copy

```
Set-LapsADReadPasswordPermission
   [-Credential <PSCredential>]
   -Identity <String[]>
   -AllowedPrincipals <String[]>
   [-Domain <String>]
   [-DomainController <String>]
   [-WhatIf]
   [-Confirm]
   [<CommonParameters>]
```

Description

The `Set-LapsADReadPasswordPermission` cmdlet is used by administrators to configure security permissions on an OU to allow specific users or groups to query LAPS passwords on computers in that OU. Users and groups must be fully qualified with both domain and user name components. The only exception to this is when the specified name resolves to a built-in principal, such as `Domain Admins`.

Examples

Example 1

PowerShell Copy

```
Set-LapsADReadPasswordPermission -Identity LapsTestOU -AllowedPrincipals "Domain Admins"


Name       DistinguishedName
----       -----------------
LapsTestOU OU=LapsTestOU,DC=laps,DC=com
```

This example shows how to run the cmdlet with an isolated name that successfully maps to a well-known user or group.

Example 2

PowerShell Copy

```
Set-LapsADReadPasswordPermission -Identity LapsTestOU -AllowedPrincipals @("S-1-5-21-2889755270-1324585639-743026605-1215")


Name       DistinguishedName
----       -----------------
LapsTestOU OU=LapsTestOU,DC=laps,DC=com
```

This example shows how to run the cmdlet specifying a user SID as input.

Example 3

PowerShell Copy

```
Set-LapsADReadPasswordPermission -Identity 'OU=LapsTestOU,DC=laps,DC=com' -AllowedPrincipals @("laps.com\LapsAdmin1", "LapsAdmin2@laps.com")


Name       DistinguishedName
----       -----------------
LapsTestOU OU=LapsTestOU,DC=laps,DC=com
```

This example shows how to run the cmdlet specifying two fully qualified user names in different formats.

Example 4

PowerShell Copy

```
Set-LapsADReadPasswordPermission -Identity LapsTestOU -AllowedPrincipals @("LapsAdministratorsGroup")


Set-LapsADReadPasswordPermission : The 'LapsAdministratorsGroup' account appears to be an isolated
name but is not a well-known name. Please use a fully qualified name instead, such as
"LAPSAdmins@contoso.com" or "contoso\LAPSAdmins"
At line:1 char:1
+ Set-LapsADReadPasswordPermission -Identity LapsTestOU -AllowedPrincip ...
+
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~
    + CategoryInfo          : InvalidArgument: (:) [Set-LapsADReadPasswordPermission], LapsPowershellException
    + FullyQualifiedErrorId : Invalid principal
specified,Microsoft.Windows.LAPS.SetLapsADReadPasswordPermission
```

This example shows a failure caused by specifying an isolated name that didn't resolve to a well-known or built-in account. The fix for this error would be to add a domain name qualifier to the input name, for example `LapsAdministratorsGroup@laps.com`.

Parameters

-AllowedPrincipals

Specifies the name of the users or groups should be granted the permissions. Users or groups may be specified in either name or SID format. If specified in name format, the name must always include the identifying domain name portion unless the name maps to a well-known or built-in account.

Expand table

Type:	String[]
Position:	Named
Default value:	None
Required:	True
Accept pipeline input:	False
Accept wildcard characters:	False

-Confirm

Prompts you for confirmation before running the cmdlet.

Expand table

Type:	SwitchParameter
Aliases:	cf
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False

-Credential

Specifies the credentials to use when updating AD. If not specified, the current user's credentials are used.

Expand table

Type:	PSCredential
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False

-Domain

Specifies the name of the domain to connect to.

Expand table

Type:	String
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False

-DomainController

Specifies the name of the domain controller to connect to.

Expand table

Type:	String

Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False

-Identity

Specifies the name of the OU to update.

This parameter accepts several different name formats that influence the criteria used in the resultant AD search. The supported name formats are as follows:

- distinguishedName (begins with a `CN=`)
- name (for all other inputs)

Setting permissions on the domain root is only supported using the distinguishedName input format, for example 'DC=laps,DC=com'.

Expand table

Type:	String[]
Position:	Named
Default value:	None
Required:	True
Accept pipeline input:	True
Accept wildcard characters:	False

-WhatIf

Shows what would happen if the cmdlet runs. The cmdlet isn't run.

Expand table

Type:	SwitchParameter
Aliases:	wi
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False

Inputs

String[]

Outputs

Object

Related Links

- Windows LAPS Overview

Revision #1
Created 5 January 2024 05:48:51 by ColtM
Updated 13 June 2024 01:28:01 by ColtM