Microsoft Exchange Server용 SnapCenter 플러그인을 설치합니다

SnapCenter Software 4.6

NetApp
January 18, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/snapcenter-46/protect-sce/concept_install_snapcenter_plug_in_for_microsoft_exchange_server.html on January 18, 2024. Always check docs.netapp.com for the latest.

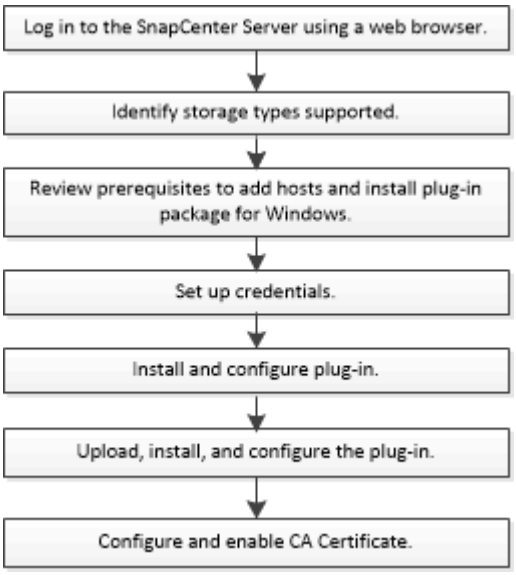
목차

Microsoft Exchange Server용 SnapCenter 플러그인을 설치합니다 . . . 1
- Microsoft Exchange Server용 SnapCenter 플러그인 설치 워크플로우 . . . 1
- 호스트를 추가하고 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하기 위한 사전 요구 사항 . . . 1
- Windows용 SnapCenter 플러그인의 자격 증명을 설정합니다 . . . 4
- Windows Server 2012 이상에서 GMSA를 구성합니다 . . . 6
- 호스트를 추가하고 Exchange용 플러그인을 설치합니다 . . . 7
- PowerShell cmdlet을 사용하여 SnapCenter Server 호스트에서 Exchange용 플러그인을 설치합니다 . . . 12
- 명령줄에서 Exchange용 SnapCenter 플러그인을 자동으로 설치합니다 . . . 13
- SnapCenter 플러그인 패키지 설치 상태를 모니터링합니다 . . . 14
- CA 인증서를 구성합니다 . . . 15
- Exchange 및 SnapCenter에 대해 SnapManager 7.x가 공존하도록 구성합니다 . . . 18

Microsoft Exchange Server용 SnapCenter 플러그인을 설치합니다

Microsoft Exchange Server용 SnapCenter 플러그인 설치 워크플로우

Exchange 데이터베이스를 보호하려면 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하고 설정해야 합니다.



호스트를 추가하고 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하기 위한 사전 요구 사항

호스트를 추가하고 플러그인 패키지를 설치하기 전에 모든 요구 사항을 완료해야 합니다.

- iSCSI를 사용하는 경우 iSCSI 서비스가 실행 중이어야 합니다.
- 원격 호스트에 대한 로컬 로그인 권한이 있는 로컬 관리자 권한이 있는 도메인 사용자가 있어야 합니다.
- 독립 실행형 및 데이터베이스 가용성 그룹 구성에 Microsoft Exchange Server 2013, 2016 또는 2019를 사용해야 합니다.
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자의 경우 호스트에서 UAC를 비활성화해야 합니다.
- SnapCenter에서 클러스터 노드를 관리하는 경우 클러스터의 모든 노드에 대한 관리 권한이 있는 사용자가 있어야 합니다.
- Exchange Server에 대한 관리 권한이 있는 사용자가 있어야 합니다.
- SnapManager for Microsoft Exchange Server 및 SnapDrive for Windows가 이미 설치되어 있는 경우, 동일한 Exchange Server에 Exchange용 플러그인을 설치하기 전에 SnapDrive for Windows에서 사용하는 VSS 하드웨어 공급자를 등록 취소해야 SnapCenter를 사용하여 데이터를 성공적으로 보호할 수 있습니다.
- Microsoft Exchange Server용 SnapManager와 Exchange용 플러그인이 동일한 서버에 설치되어 있는 경우

Windows 스케줄러에서 Microsoft Exchange Server용 SnapManager가 생성한 모든 스케줄을 일시 중지하거나 삭제해야 합니다.

- 호스트는 서버에서 FQDN(정규화된 도메인 이름)으로 확인할 수 있어야 합니다. 호스트 파일을 확인할 수 있도록 수정하고 호스트 파일에 짧은 이름과 FQDN이 모두 지정된 경우 *<IP_address><host_FQDN><host_name>* 형식으로 SnapCenter hosts 파일에 항목을 생성합니다.
- 방화벽에서 다음 포트가 차단되지 않았는지 확인합니다. 차단되지 않으면 호스트 추가 작업이 실패합니다. 이 문제를 해결하려면 동적 포트 범위를 구성해야 합니다. 자세한 내용은 을 참조하십시오 "Microsoft 설명서".
  - Windows 2016 및 Exchange 2016의 경우 포트 범위 50000 - 51000
  - Windows 2012 R2 및 Exchange 2013의 경우 포트 범위는 6000-6500입니다
  - Windows 2019의 경우 포트 범위 49152-65536

포트 범위를 식별하려면 다음 명령을 실행합니다.

- netsh int ipv4 show dynamicport tcp
- netsh int ipv4 show dynamicport udp
- netsh int ipv6 show dynamicport tcp
- netsh int ipv6 show dynamicport UDP

Windows용 SnapCenter 플러그인 패키지를 설치하기 위한 호스트 요구 사항

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항 및 사이징 요구 사항을 숙지해야 합니다.

항목	요구 사항
운영 체제	Microsoft Windows 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.

항목	요구 사항
필요한 소프트웨어 패키지	• Microsoft .NET Framework 4.5.2 이상 • WMF(Windows Management Framework) 4.0 이상 • PowerShell 4.0 이상 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

Exchange Server 권한이 필요합니다

SnapCenter에서 Exchange Server 또는 DAG를 추가하고 호스트 또는 DAG에 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하려면 최소 권한 및 권한 세트가 있는 사용자에 대한 자격 증명을 사용하여 SnapCenter를 구성해야 합니다.

로컬 관리자 권한이 있는 도메인 사용자와 원격 Exchange 호스트에 대한 로컬 로그인 권한, DAG의 모든 노드에 대한 관리 권한이 있어야 합니다. 도메인 사용자에게는 다음과 같은 최소 권한이 필요합니다.

- Add-MailboxDatabaseCopy 를 선택합니다
- 마운트 해제 - 데이터베이스
- 가져오기 - AdServerSettings
- Get-DatabaseAvailabilityGroup
- Get-ExchangeServer를 선택합니다
- Get-MailboxDatabase
- Get-MailboxDatabaseCopyStatus 를 참조하십시오
- Get-MailboxServer 를 참조하십시오
- Get-MailboxStatistics를 참조하십시오
- Get-PublicFolderDatabase를 참조하십시오
- Move-ActiveMailboxDatabase(ActiveMailboxDatabase 이동)
- move-DatabasePath-ConfigurationOnly:$true입니다
- 마운트 - 데이터베이스
- New - MailboxDatabase
- 새 기능 - PublicFolderDatabase
- remove - MailboxDatabase(메일 사서함 데이터베이스)
- remove-MailboxDatabaseCopy 를 선택합니다
- 제거 - PublicFolderDatabase
- Resume - MailboxDatabaseCopy
- 설정 - AdServerSettings
- Set-MailboxDatabase -allowfilerestore:$true입니다

- Set-MailboxDatabaseCopy 를 선택합니다
- Set-PublicFolderDatabase
- Suspend-MailboxDatabaseCopy 를 선택합니다
- 업데이트 - MailboxDatabaseCopy

Windows Server 2012 이상에서 GMSA를 구성합니다

Windows용 SnapCenter 플러그인 패키지를 설치하기 전에 몇 가지 기본적인 호스트 시스템 공간 요구 사항 및 사이징 요구 사항을 숙지해야 합니다.

항목	요구 사항
운영 체제	Microsoft Windows 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".
호스트의 SnapCenter 플러그인에 대한 최소 RAM입니다	1GB
호스트의 SnapCenter 플러그인에 대한 최소 설치 및 로그 공간	5GB 충분한 디스크 공간을 할당하고 로그 폴더의 스토리지 사용량을 모니터링해야 합니다. 필요한 로그 공간은 보호할 엔터티의 수와 데이터 보호 작업의 빈도에 따라 달라집니다. 디스크 공간이 충분하지 않으면 최근 실행 작업에 대한 로그가 생성되지 않습니다.
필요한 소프트웨어 패키지	• Microsoft .NET Framework 4.5.2 이상 • WMF(Windows Management Framework) 4.0 이상 • PowerShell 4.0 이상 지원되는 버전에 대한 최신 정보는 를 참조하십시오 "NetApp 상호 운용성 매트릭스 툴".

Windows용 SnapCenter 플러그인의 자격 증명을 설정합니다

SnapCenter는 자격 증명을 사용하여 SnapCenter 작업을 위해 사용자를 인증합니다. 플러그인 패키지를 설치하기 위한 자격 증명과 데이터베이스에서 데이터 보호 작업을 수행하기 위한 추가 자격 증명을 만들어야 합니다.

- 이 작업에 대한 정보 *

Windows 호스트에 플러그인을 설치하기 위한 자격 증명을 설정해야 합니다. 호스트를 구축하고 플러그인을 설치한 후

Windows에 대한 자격 증명을 생성할 수 있지만, 호스트를 구축하고 플러그인을 설치하기 전에 SVM을 추가한 후에 자격 증명을 생성하는 것이 가장 좋습니다.

원격 호스트에 대한 관리자 권한을 포함하여 관리자 권한으로 자격 증명을 설정합니다.

개별 리소스 그룹에 대한 자격 증명을 설정했고 사용자 이름에 전체 관리자 권한이 없는 경우 최소한 리소스 그룹 및 백업 권한을 사용자 이름에 할당해야 합니다.

- 단계 *

1. 왼쪽 탐색 창에서 * 설정 * 을 클릭합니다.
2. 설정 페이지에서 * 자격 증명 * 을 클릭합니다.
3. 새로 만들기 * 를 클릭합니다.

   자격 증명 창이 표시됩니다.

4. 자격 증명 페이지에서 다음을 실행합니다.

이 필드의 내용...	수행할 작업...
자격 증명 이름입니다	자격 증명의 이름을 입력합니다.
사용자 이름	인증에 사용되는 사용자 이름을 입력합니다. • 도메인 관리자 또는 관리자 그룹의 구성원 SnapCenter 플러그인을 설치할 시스템의 도메인 관리자 또는 관리자 그룹의 구성원을 지정합니다. 사용자 이름 필드에 유효한 형식은 다음과 같습니다. ◦ 'NetBIOS\사용자 이름' ◦ Domain FQDN\username’입니다 • 로컬 관리자(작업 그룹에만 해당) 작업 그룹에 속한 시스템의 경우 SnapCenter 플러그인을 설치할 시스템에 기본 제공 로컬 관리자를 지정합니다. 사용자 계정에 상승된 권한이 있거나 호스트 시스템에서 사용자 액세스 제어 기능이 비활성화된 경우 로컬 관리자 그룹에 속하는 로컬 사용자 계정을 지정할 수 있습니다. 사용자 이름 필드의 올바른 형식은 '사용자 이름 ’입니다
암호	인증에 사용되는 암호를 입력합니다.
인증	인증 모드로 Windows를 선택합니다.

5. 확인 * 을 클릭합니다.

Windows Server 2012 이상에서 GMSA를 구성합니다

Windows Server 2012 이상을 사용하면 관리되는 도메인 계정에서 자동화된 서비스 계정 암호 관리를 제공하는 그룹 GMSA(Managed Service Account)를 만들 수 있습니다.

- 필요한 것 *
- Windows Server 2012 이상의 도메인 컨트롤러가 있어야 합니다.
- 도메인의 구성원인 Windows Server 2012 이상 호스트가 있어야 합니다.
- 단계 *

1. KDS 루트 키를 생성하여 GMSA의 각 개체에 대해 고유한 암호를 생성합니다.
2. 각 도메인에 대해 Windows 도메인 컨트롤러에서 Add-KDSRootKey-EffectiveImmediately 명령을 실행합니다
3. GMSA 생성 및 구성:
   a. 다음 형식으로 사용자 그룹 계정을 만듭니다.

```
 domainName\accountName$
.. 그룹에 컴퓨터 개체를 추가합니다.
.. 방금 생성한 사용자 그룹을 사용하여 GMSA를 생성합니다.
```

   예를 들면, 다음과 같습니다.

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName
<fqdn> -PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Get-ADServiceAccount 명령을 실행하여 서비스 계정을 확인한다.
```

4. 호스트에서 GMSA를 구성합니다.
   a. GMSA 계정을 사용할 호스트에서 Windows PowerShell용 Active Directory 모듈을 활성화합니다.

      이렇게 하려면 PowerShell에서 다음 명령을 실행합니다.

```
PS C:\> Get-WindowsFeature AD-Domain-Services

Display Name                                Name                Install State
------------                                ----                -------------
[ ] Active Directory Domain Services   AD-Domain-Services  Available


PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Active Directory Domain Services,
Active ...
WARNING: Windows automatic updating is not enabled. To ensure that your
newly-installed role or feature is
automatically updated, turn on Windows Update.
```

a. 호스트를 다시 시작합니다.

b. PowerShell 명령 프롬프트에서 'Install-AdServiceAccount<GMSA>'를 실행하여 호스트에 GMSA를 설치합니다

c. 'Test-AdServiceAccount <GMSA>' 명령을 실행하여 GMSA 계정을 확인합니다

   1. 호스트에서 구성된 GMSA에 관리 권한을 할당합니다.
   2. SnapCenter 서버에서 구성된 GMSA 계정을 지정하여 Windows 호스트를 추가합니다.

      SnapCenter 서버는 선택한 플러그인을 호스트에 설치하고 지정된 GMSA는 플러그인 설치 중에 서비스 로그온 계정으로 사용됩니다.

호스트를 추가하고 **Exchange**용 플러그인을 설치합니다

SnapCenter 호스트 추가 페이지를 사용하여 Windows 호스트를 추가할 수 있습니다. Exchange용 플러그인은 지정된 호스트에 자동으로 설치됩니다. 이는 플러그인을 설치하는 데 권장되는 방법입니다. 호스트를 추가하고 개별 호스트 또는 클러스터에 대한 플러그인을 설치할 수 있습니다.

- 필요한 것 *
- 플러그인 설치 및 제거 권한이 있는 역할(예: SnapCenter 관리자)에 할당된 사용자여야 합니다
- Windows 호스트에 플러그인을 설치할 때 기본 제공되지 않은 자격 증명을 지정하거나 사용자가 로컬 작업 그룹 사용자에 속한 경우 호스트에서 UAC를 비활성화해야 합니다.
- 메시지 큐 서비스가 실행되고 있어야 합니다.
- 그룹 GMSA(Managed Service Account)를 사용하는 경우 관리자 권한으로 GMSA를 구성해야 합니다. 자세한 내용은 을 참조하십시오"Microsoft Exchange Server에 대해 Windows Server 2012 이상에서 그룹 관리 서비스 계정을 구성합니다".

- 이 작업에 대한 정보 *
- SnapCenter 서버를 다른 SnapCenter 서버에 플러그인 호스트로 추가할 수 없습니다.
- 호스트를 추가하고 개별 호스트 또는 클러스터에 대한 플러그인 패키지를 설치할 수 있습니다.
- Exchange 노드가 DAG의 일부인 경우 SnapCenter 서버에 하나의 노드만 추가할 수 없습니다.
- 클러스터(Exchange DAG)에 플러그인을 설치하는 경우 일부 노드에 NetApp LUN에 데이터베이스가 없는 경우에도 클러스터의 모든 노드에 플러그인이 설치됩니다.

SnapCenter 4.6부터 SCE는 멀티 테넌시를 지원하며 다음 방법을 사용하여 호스트를 추가할 수 있습니다.

호스트 작업을 추가합니다	**4.5** 이하	**4.6** 이상
크로스 또는 다른 도메인에 IP-less DAG를 추가합니다	지원되지 않습니다	지원
동일한 도메인 또는 교차 도메인에 있는 고유한 이름의 여러 IP DAG를 추가합니다	지원	지원
도메인 간에 동일한 호스트 이름 및 /또는 DB 이름을 가진 여러 IP 또는 IP가 없는 DAG를 추가합니다	지원되지 않습니다	지원
동일한 이름과 도메인 간에 여러 IP/IP 없는 DAG를 추가합니다	지원되지 않습니다	지원
동일한 이름과 도메인 간에 여러 독립 실행형 호스트를 추가합니다	지원되지 않습니다	지원

Exchange용 플러그인은 Windows용 SnapCenter 플러그인 패키지에 따라 다르며 버전이 같아야 합니다. Exchange용 플러그인 설치 중에 Windows용 SnapCenter 플러그인 패키지가 기본적으로 선택되어 있으며 VSS 하드웨어 공급자와 함께 설치됩니다.

Microsoft Exchange Server용 SnapManager와 Windows용 SnapDrive가 이미 설치되어 있는 경우 Exchange용 플러그인을 동일한 Exchange Server에 설치하려면 Exchange용 플러그인 및 Windows용 SnapCenter 플러그인 패키지와 함께 설치된 VSS 하드웨어 공급자와 호환되지 않으므로 Windows용 SnapDrive에서 사용하는 VSS 하드웨어 공급자를 등록 취소해야 합니다. 자세한 내용은 을 참조하십시오 "Data ONTAP VSS 하드웨어 공급자를 수동으로 등록하는 방법".

- 단계 *

1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
2. 맨 위에 * Managed Hosts * 가 선택되어 있는지 확인합니다.
3. 추가 * 를 클릭합니다.
4. 호스트 페이지에서 다음을 수행합니다.

이 필드의 내용...	수행할 작업...
호스트 유형	호스트 유형으로 * Windows * 를 선택합니다. SnapCenter 서버는 호스트를 추가한 다음 호스트에 Windows용 플러그인 및 Exchange용 플러그인이 설치되어 있지 않은 경우 호스트에 설치합니다. Windows용 플러그인과 Exchange용 플러그인은 동일한 버전이어야 합니다. 다른 버전의 Windows용 플러그인이 이전에 설치된 경우 SnapCenter는 설치 과정에서 버전을 업데이트합니다.

이 필드의 내용...	수행할 작업...
호스트 이름입니다	FQDN(정규화된 도메인 이름) 또는 호스트의 IP 주소를 입력합니다. SnapCenter는 DNS의 올바른 구성에 따라 달라집니다. 따라서 가장 좋은 방법은 FQDN(정규화된 도메인 이름)을 입력하는 것입니다. IP 주소는 FQDN으로 확인되는 경우에만 신뢰할 수 없는 도메인 호스트에 대해 지원됩니다. SnapCenter를 사용하여 호스트를 추가하고 이 호스트가 하위 도메인의 일부인 경우 FQDN을 제공해야 합니다. 다음 중 하나의 IP 주소 또는 FQDN을 입력할 수 있습니다. • 독립 실행형 호스트 • Exchange DAG Exchange DAG의 경우 다음을 수행할 수 있습니다. ◦ DAG 이름, DAG IP 주소, 노드 이름 또는 노드 IP 주소를 제공하여 DAG를 추가합니다. ◦ DAG 클러스터 노드 중 하나의 IP 주소 또는 FQDN을 제공하여 IP less DAG 클러스터를 추가합니다. ◦ 동일한 도메인 또는 다른 도메인에 상주하는 IP가 적은 DAG를 추가합니다. 이름은 같지만 도메인이 다른 여러 IP/IP가 없는 DAG를 추가할 수도 있습니다. ⓘ 독립 실행형 호스트 또는 Exchange DAG(도메인 간 또는 동일한 도메인)의 경우 호스트 또는 DAG의 IP 주소 또는 FQDN을 제공하는 것이 좋습니다.

이 필드의 내용...	수행할 작업...
자격 증명	생성한 자격 증명 이름을 선택하거나 새 자격 증명을 생성합니다. 자격 증명에 원격 호스트에 대한 관리 권한이 있어야 합니다. 자세한 내용은 자격 증명 만들기에 대한 정보를 참조하십시오. 지정한 자격 증명 이름 위에 커서를 놓으면 자격 증명에 대한 세부 정보를 볼 수 있습니다. 자격 증명 인증 모드는 호스트 추가 마법사에서 지정하는 호스트 유형에 의해 결정됩니다.

5. 설치할 플러그인 선택 섹션에서 설치할 플러그인을 선택합니다.

   Exchange용 플러그인을 선택하면 Microsoft SQL Server용 SnapCenter 플러그인 선택이 자동으로 취소됩니다. 사용된 메모리 양과 Exchange에 필요한 기타 리소스 사용 때문에 SQL Server와 Exchange Server를 동일한 시스템에 설치하지 않는 것이 좋습니다.

6. (선택 사항) * 추가 옵션 * 을 클릭합니다.

이 필드의 내용...	수행할 작업...
포트	기본 포트 번호를 유지하거나 포트 번호를 지정합니다. 기본 포트 번호는 8145입니다. SnapCenter 서버가 사용자 지정 포트에 설치된 경우 해당 포트 번호가 기본 포트로 표시됩니다. 플러그인을 수동으로 설치하고 사용자 지정 포트를 지정한 경우 동일한 포트를 지정해야 합니다. 그렇지 않으면 작업이 실패합니다.
설치 경로	기본 경로는 'C:\Program Files\NetApp\SnapCenter'입니다. 선택적으로 경로를 사용자 지정할 수 있습니다.
DAG의 모든 호스트를 추가합니다	DAG를 추가할 때 이 확인란을 선택합니다.
사전 설치 검사를 건너뜁니다	플러그인이 이미 수동으로 설치되어 있고 호스트가 플러그인 설치 요구 사항을 충족하는지 확인하지 않으려면 이 확인란을 선택합니다.

이 필드의 내용...	수행할 작업...
그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행합니다	그룹 GMSA(Managed Service Account)를 사용하여 플러그인 서비스를 실행하려면 이 확인란을 선택합니다. GMSA 이름을 *domainName\accountName$* 형식으로 제공합니다. GMSA는 SnapCenter Plug-in for Windows 서비스에 대해서만 로그온 서비스 계정으로 사용됩니다.

7. 제출 * 을 클릭합니다.

   사전 검사 건너뛰기 확인란을 선택하지 않은 경우 호스트가 플러그인을 설치하기 위한 요구사항을 충족하는지 여부를 확인합니다. 최소 요구 사항이 충족되지 않으면 적절한 오류 또는 경고 메시지가 표시됩니다.

   이 오류가 디스크 공간 또는 RAM과 관련된 경우 'C:\Program Files\NetApp\SnapCenter' WebApp에 있는 web.config 파일을 업데이트하여 기본값을 수정할 수 있습니다. 오류가 다른 매개변수와 관련된 경우 문제를 해결해야 합니다.

   HA 설정에서 web.config 파일을 업데이트하는 경우 두 노드에서 파일을 업데이트해야 합니다.

1. 설치 과정을 모니터링합니다.

PowerShell cmdlet을 사용하여 SnapCenter Server 호스트에서 Exchange용 플러그인을 설치합니다

SnapCenter GUI에서 Exchange용 플러그인을 설치해야 합니다. GUI를 사용하지 않으려는 경우 SnapCenter 서버 호스트 또는 원격 호스트에서 PowerShell cmdlet을 사용할 수 있습니다.

- 필요한 것 *
- SnapCenter 서버가 설치 및 구성되어 있어야 합니다.
- 호스트 또는 관리 권한이 있는 사용자의 로컬 관리자여야 합니다.
- 플러그인, 설치 및 제거 권한이 있는 역할(예: SnapCenter 관리자)에 할당된 사용자여야 합니다
- Exchange용 플러그인을 설치하기 전에 설치 요구 사항 및 지원되는 구성 유형을 검토해야 합니다.
- Exchange용 플러그인을 설치할 호스트는 Windows 호스트여야 합니다.
- 단계 *

1. SnapCenter 서버 호스트에서 _Open-SmConnection_cmdlet을 사용하여 세션을 설정한 다음 자격 증명을 입력합니다.
2. 필요한 매개 변수와 함께 _Add-SmHost_cmdlet을 사용하여 Exchange용 플러그인을 설치할 호스트를 추가합니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

호스트는 독립 실행형 호스트 또는 DAG일 수 있습니다. DAG를 지정하는 경우 _-IsDAG_매개 변수가 필요합니다.

1. 필요한 매개 변수와 함께 _Install-SmHostPackage_cmdlet을 사용하여 Exchange용 플러그인을 설치합니다.

   이 명령은 지정된 호스트에 Exchange용 플러그인을 설치한 다음 SnapCenter에 플러그인을 등록합니다.

명령줄에서 **Exchange**용 **SnapCenter** 플러그인을 자동으로 설치합니다

SnapCenter 사용자 인터페이스 내에서 Exchange용 플러그인을 설치해야 합니다. 그러나 어떤 이유로 인해 Windows 명령줄에서 자동 모드로 Exchange용 플러그인 설치 프로그램을 실행할 수 없습니다.

- 필요한 것 *
- Microsoft Exchange Server 리소스를 백업해야 합니다.
- SnapCenter 플러그인 패키지를 설치해야 합니다.
- 설치하기 전에 Microsoft SQL Server용 SnapCenter 플러그인의 이전 릴리즈를 삭제해야 합니다.

  자세한 내용은 을 참조하십시오 "플러그인 호스트에서 직접 SnapCenter 플러그인을 설치하는 방법".

- 단계 *

1. 플러그인 호스트에 _C:\temp_folder가 있고 로그인한 사용자가 이 폴더에 대한 모든 액세스 권한을 가지고 있는지 확인합니다.
2. C:\ProgramData\NetApp\SnapCenter\Package_Repository에서 Microsoft Windows용 SnapCenter 플러그인을 다운로드하십시오.

   이 경로는 SnapCenter 서버가 설치된 호스트에서 액세스할 수 있습니다.

3. 플러그인을 설치할 호스트에 설치 파일을 복사합니다.
4. 로컬 호스트의 Windows 명령 프롬프트에서 플러그인 설치 파일을 저장한 디렉토리로 이동합니다.
5. 다음 명령을 입력하여 변수가 데이터로 교체되도록 설치합니다.

   _snapcenter_windows_host_plugin.exe" /silent/debuglog"<Debug_Log_Path>"/log"<Log_Path>"BI_SNAPCENTER_PORT=<Num>Suite_INSTALLDIR="<Install_Directory_Path>"BI_ServiceAccount=<domain\administrator>BI_SERVICEPSCE=<설치 암호>

   예를 들면 다음과 같습니다.

   _C:\ProgramData\NetApp\SnapCenter\Package Repository\snapcenter_windows_host_plugin.exe" /silent/debuglog "C:\HPPW_SCSQL_Install.log" /log" C:\temp "BI_SNAPCENTER_port=8145 Suite_INSTALLDIR="C:\Program Files\NetApp\SCVICE_PVICE.PCEWE_PCEBI 관리자, PVICE_PVICE_PCEWESTRW=PCEBI_PCEPCEPCEWE_PSHI=설치

Exchange용 플러그인을 설치하는 동안 전달되는 모든 매개 변수는 대/소문자를 구분합니다.

a. _/silent/debuglog "C:\Installdebug.log" /log "C:\temp" BI_SNAPCENTER_PORT=8145 Suite_INSTALLDIR="C:\Program Files" BI_ServiceAccount=demo\administrator BI_SERVICEPWD=Netapp1! ISFeatureInstall = HPPW, SCW _

변수에 대해 다음 값을 입력합니다.

변수	값
_ /debuglog "<Debug_Log_Path> _	다음 예제와 같이 제품군 설치 관리자 로그 파일의 이름과 위치를 지정합니다. *Setup.exe /debuglog "C:\PathToLog\setupexe.log*
Bi_SNAPCENTER_PORT	SnapCenter가 SMCore와 통신하는 포트를 지정합니다.
Suite_INSTALLDIR	호스트 플러그인 패키지 설치 디렉토리를 지정합니다.
BI_서비스 계정	Microsoft Windows 웹 서비스 계정용 SnapCenter 플러그인을 지정합니다.
BI_세비셀	Microsoft Windows 웹 서비스 계정용 SnapCenter 플러그인 암호를 지정합니다.
ISFeatureInstall을 선택합니다	SnapCenter가 원격 호스트에 구축할 솔루션을 지정합니다.

1. Windows 작업 스케줄러, 기본 설치 로그 파일 *C:\Installdebug.log* 및 추가 설치 파일을 _C:\Temp_에서 모니터링합니다.
2. %temp%_ 디렉토리를 모니터링하여 _msiexe.exe_설치 프로그램이 오류 없이 소프트웨어를 설치하고 있는지 확인합니다.

Exchange용 플러그인을 설치하면 SnapCenter 서버가 아닌 호스트에 플러그인이 등록됩니다. SnapCenter GUI 또는 PowerShell cmdlet을 사용하여 호스트를 추가하여 SnapCenter 서버에 플러그인을 등록할 수 있습니다. 호스트가 추가되면 플러그인이 자동으로 검색됩니다.

SnapCenter 플러그인 패키지 설치 상태를 모니터링합니다

작업 페이지를 사용하여 SnapCenter 플러그인 패키지 설치 진행률을 모니터링할 수 있습니다. 설치 진행 상황을 확인하여 설치 완료 시기 또는 문제가 있는지 확인할 수 있습니다.

- 이 작업에 대한 정보 *

작업 페이지에 다음 아이콘이 나타나고 작업의 상태를 나타냅니다.

- 진행 중입니다
- 성공적으로 완료되었습니다
- 실패했습니다
- 경고와 함께 완료되었거나 경고로 인해 시작할 수 없습니다
- 대기열에 있습니다
- 단계 *
  1. 왼쪽 탐색 창에서 * 모니터 * 를 클릭합니다.
  2. 모니터 페이지에서 * 작업 * 을 클릭합니다.
  3. 작업 페이지에서 플러그인 설치 작업만 나열되도록 목록을 필터링하려면 다음을 수행합니다.
     a. 필터 * 를 클릭합니다.
     b. 선택 사항: 시작 및 종료 날짜를 지정합니다.
     c. 유형 드롭다운 메뉴에서 * 플러그인 설치 * 를 선택합니다.
     d. 상태 드롭다운 메뉴에서 설치 상태를 선택합니다.
     e. 적용 * 을 클릭합니다.
  4. 설치 작업을 선택하고 * 세부 정보 * 를 클릭하여 작업 세부 정보를 봅니다.
  5. 작업 세부 정보 페이지에서 * 로그 보기 * 를 클릭합니다.

CA 인증서를 구성합니다

CA 인증서 CSR 파일을 생성합니다

CSR(인증서 서명 요청)을 생성하고 생성된 CSR을 사용하여 CA(인증 기관)에서 가져올 수 있는 인증서를 가져올 수 있습니다. 인증서에 연결된 개인 키가 있습니다.

CSR은 서명된 CA 인증서를 조달하기 위해 공인 인증서 공급업체에 제공되는 인코딩된 텍스트 블록입니다.

CSR 생성에 대한 자세한 내용은 을 참조하십시오 "CA 인증서 CSR 파일을 생성하는 방법".

> 도메인(* .domain.company.com) 또는 시스템(machine1.domain.company.com CA 인증서를 소유하고 있는 경우 CA 인증서 CSR 파일 생성을 건너뛸 수 있습니다. SnapCenter를 사용하여 기존 CA 인증서를 배포할 수 있습니다.

클러스터 구성의 경우 클러스터 이름(가상 클러스터 FQDN) 및 해당 호스트 이름을 CA 인증서에 언급해야 합니다. 인증서를 조달하기 전에 SAN(Subject Alternative Name) 필드를 채워 인증서를 업데이트할 수 있습니다. 와일드카드 인증서(* .domain.company.com)의 경우 인증서에 도메인의 모든 호스트 이름이 암시적으로 포함됩니다.

CA 인증서를 가져옵니다

MMC(Microsoft Management Console)를 사용하여 CA 인증서를 SnapCenter 서버 및 Windows 호스트 플러그인으로 가져와야 합니다.

- 단계 *

1. MMC(Microsoft Management Console)로 이동한 다음 * 파일 * > * Snapin 추가/제거 * 를 클릭합니다.
2. 스냅인 추가/제거 창에서 * 인증서 * 를 선택한 다음 * 추가 * 를 클릭합니다.
3. 인증서 스냅인 창에서 * 컴퓨터 계정 * 옵션을 선택한 다음 * 마침 * 을 클릭합니다.
4. 콘솔 루트 * > * 인증서 – 로컬 컴퓨터 * > * 신뢰할 수 있는 루트 인증 기관 * > * 인증서 * 를 클릭합니다.
5. "신뢰할 수 있는 루트 인증 기관" 폴더를 마우스 오른쪽 단추로 클릭한 다음 * 모든 작업 * > * 가져오기 * 를 선택하여 가져오기 마법사를 시작합니다.
6. 다음과 같이 마법사를 완료합니다.

이 마법사 창에서...	다음을 수행합니다.
개인 키를 가져옵니다	예 * 옵션을 선택하고 개인 키를 가져온 다음 * 다음 * 을 클릭합니다.
파일 형식 가져오기	변경하지 않고 * 다음 * 을 클릭합니다.
보안	내보낸 인증서에 사용할 새 암호를 지정하고 * 다음 * 을 클릭합니다.
인증서 가져오기 마법사 완료	요약을 검토한 후 * Finish * 를 클릭하여 가져오기를 시작합니다.

인증서 가져오기는 개인 키와 함께 번들로 제공됩니다(지원되는 형식은 *.pfx, *.p12, *.p7b).

7. "개인" 폴더에 대해 5단계를 반복합니다.

CA 인증서 지문을 받습니다

인증서 thumbprint는 인증서를 식별하는 16진수 문자열입니다. 썸프린트는 썸프린트 알고리즘을 사용하여 인증서 컨텐츠에서 계산됩니다.

- 단계 *

1. GUI에서 다음을 수행합니다.
   a. 인증서를 두 번 클릭합니다.
   b. 인증서 대화 상자에서 * 세부 정보 * 탭을 클릭합니다.
   c. 필드 목록을 스크롤하여 * Thumbprint * 를 클릭합니다.
   d. 상자에서 16진수 문자를 복사합니다.
   e. 16진수 사이의 공백을 제거합니다.

   예를 들어, 썸프린트가 "A9 09 50 2D D8 2a E4 14 33 E6 F8 38 86 b0 0d 42 77 A3 2a 7b"인 경우 공백을 제거한 후 "a909502dd82ae41433e6f83886b00d4277a32a7b"가 됩니다.

2. PowerShell에서 다음을 수행합니다.

a. 다음 명령을 실행하여 설치된 인증서의 엄지손가락 지문을 나열하고 최근 설치된 인증서를 주체 이름으로 식별합니다.

Get-ChildItem-Path 인증:*LocalMachine**My*

b. 엄지손가락 지문을 복사합니다.

Windows 호스트 플러그인 서비스를 사용하여 CA 인증서를 구성합니다

설치된 디지털 인증서를 활성화하려면 Windows 호스트 플러그인 서비스를 사용하여 CA 인증서를 구성해야 합니다.

SnapCenter 서버 및 CA 인증서가 이미 배포된 모든 플러그인 호스트에서 다음 단계를 수행합니다.

- 단계 *

1. 다음 명령을 실행하여 SMCore 기본 포트 8145를 사용하여 기존 인증서 바인딩을 제거합니다.

">netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>"를 선택합니다

예를 들면 다음과 같습니다.

```
 > netsh http delete sslcert ipport=0.0.0.0:8145
. 다음 명령을 실행하여 새로 설치된 인증서를 Windows 호스트 플러그인 서비스와 바인딩합니다.
```

">$cert="<*certificate thumbprint*>"

'>$GUID=[GUID]::NewGuid().ToString("B")'

">netsh http add sslcert ipport=0.0.0.0:_<SMCore Port>_CertHash=$cert AppID="$GUID""

예를 들면 다음과 같습니다.

```
> $cert = “a909502dd82ae41433e6f83886b00d4277a32a7b”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert
appid="$guid"
```

플러그인에 대해 CA 인증서를 활성화합니다

CA 인증서를 구성하고 SnapCenter 서버 및 해당 플러그인 호스트에 CA 인증서를 배포해야 합니다. 플러그인에 대해 CA 인증서 유효성 검사를 활성화해야 합니다.

- 필요한 것 *
- run_Set-SmCertificateSettings_cmdlet을 사용하여 CA 인증서를 활성화하거나 비활성화할 수 있습니다.
- _get-SmCertificateSettings_를 사용하여 플러그인의 인증서 상태를 표시할 수 있습니다.

cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 running_get-Help command_name_에서 확인할 수 있습니다. 또는 을 참조할 수도 있습니다 "SnapCenter 소프트웨어 cmdlet 참조 가이드".

- 단계 *
  1. 왼쪽 탐색 창에서 * 호스트 * 를 클릭합니다.
  2. 호스트 페이지에서 * 관리되는 호스트 * 를 클릭합니다.
  3. 단일 또는 여러 플러그인 호스트를 선택합니다.
  4. 추가 옵션 * 을 클릭합니다.
  5. 인증서 유효성 검사 사용 * 을 선택합니다.
- 완료 후 *

관리 호스트 탭 호스트에는 자물쇠가 표시되고 자물쇠 색상은 SnapCenter 서버와 플러그인 호스트 간의 연결 상태를 나타냅니다.

- 는 CA 인증서가 활성화되지 않았으며 플러그인 호스트에 할당되지 않았음을 나타냅니다.
- CA 인증서의 유효성을 확인했음을 나타냅니다.
- CA 인증서의 유효성을 확인할 수 없음을 나타냅니다.
- 연결 정보를 검색할 수 없음을 나타냅니다.

상태가 노란색 또는 녹색이면 데이터 보호 작업이 성공적으로 완료된 것입니다.

Exchange 및 SnapCenter에 대해 SnapManager 7.x가 공존하도록 구성합니다

Microsoft Exchange Server용 SnapCenter 플러그인을 Microsoft Exchange Server용 SnapManager와 함께 사용하려면 Microsoft Exchange Server용 SnapManager가 설치된 동일한 Exchange Server에 Microsoft Exchange Server용 SnapCenter 플러그인을 설치하고 Exchange 일정에 대해 SnapManager를 사용하지 않도록 설정해야 합니다. 및 Microsoft Exchange Server용 SnapCenter 플러그인을 사용하여 새 일정 및 백업을 구성합니다.

- 필요한 것 *
- Microsoft Exchange Server용 SnapManager와 Windows용 SnapDrive가 이미 설치되어 있고 Microsoft Exchange Server용 SnapManager 백업이 시스템과 SnapInfo 디렉토리에 있습니다.
- 더 이상 필요하지 않은 Microsoft Exchange Server용 SnapManager에서 생성한 백업을 삭제하거나 회수해야 합니다.
- Windows 스케줄러에서 Microsoft Exchange Server용 SnapManager가 만든 모든 일정을 일시 중단하거나 삭제해야 합니다.
- Microsoft Exchange Server용 SnapCenter 플러그인과 Microsoft Exchange Server용 SnapManager가 동일한 Exchange Server에 공존할 수 있지만 기존 Microsoft Exchange Server용 SnapManager 설치를 SnapCenter로 업그레이드할 수는 없습니다.

  SnapCenter는 업그레이드 옵션을 제공하지 않습니다.

- SnapCenter는 SnapManager for Microsoft Exchange Server 백업에서 Exchange 데이터베이스 복원을 지원하지 않습니다.

  Microsoft Exchange Server용 SnapCenter 플러그인 설치 후 Microsoft Exchange Server용 SnapManager를 제거하지 않고 나중에 Microsoft Exchange Server용 SnapManager 백업을 복원하려면 추가 단계를 수행해야 합니다.

- 단계 *

  1. 모든 DAG 노드에서 PowerShell을 사용하여 SnapDrive for Windows VSS Hardware Provider가 등록되었는지 여부를 확인합니다. _ vssadmin list providers _

     ```
     C:\Program Files\NetApp\SnapDrive>vssadmin list providers
     vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
     tool
     (C) Copyright 2001-2013 Microsoft Corp.

     Provider name: 'Data ONTAP VSS Hardware Provider'
        Provider type: Hardware
        Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
        Version: 7. 1. 4. 6845
     ```

  2. SnapDrive 디렉토리에서 SnapDrive for Windows에서 VSS 하드웨어 공급자 등록을 취소합니다. *navssprv.exe -r service –u*
  3. VSS Hardware Provider가 제거되었는지 확인합니다. _ vssadmin list providers _
  4. SnapCenter에 Exchange 호스트를 추가한 다음 Microsoft Windows용 SnapCenter 플러그인 및 Microsoft Exchange Server용 SnapCenter 플러그인을 설치합니다.
  5. 모든 DAG 노드의 Microsoft Windows용 SnapCenter 플러그인 디렉토리에서 VSS 하드웨어 공급자가 등록되었는지 확인합니다. *vssadmin list providers*

     ```
     [PS] C:\Windows\system32>vssadmin list providers
     vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
     tool
     (C) Copyright 2001-2013 Microsoft Corp.

     Provider name: 'Data ONTAP VSS Hardware Provider'
        Provider type: Hardware
        Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
        Version: 7. 0. 0. 5561
     ```

  6. Microsoft Exchange Server 백업 일정에 대한 SnapManager를 중지합니다.
  7. SnapCenter GUI를 사용하여 필요 시 백업을 생성하고, 예약된 백업을 구성하고, 보존 설정을 구성합니다.
  8. Microsoft Exchange Server용 SnapManager를 제거합니다.

     Microsoft Exchange Server용 SnapManager를 지금 제거하지 않고 나중에 Microsoft Exchange Server용

SnapManager 백업을 복원하려는 경우:

a. 모든 DAG 노드에서 Microsoft Exchange Server용 SnapCenter 플러그인 등록 취소: _navssprv.exe -r service -u _

```
C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for
Microsoft Windows>navssprv.exe -r service -u
```

b. C:\Program Files\NetApp\SnapDrive_ 디렉토리에서 모든 DAG 노드에 SnapDrive for Windows를 등록합니다. _navssprv.exe -r service -a hostname \\username -p password _

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.