LDAP에 대한 Insight 구성

OnCommand Insight

NetApp
October 24, 2024

목차

LDAP에 대한 Insight 구성

OnCommand Insight는 회사 LDAP 도메인에서 구성되므로 LDAP(Lightweight Directory Access Protocol) 설정으로 구성해야 합니다.

LDAP 또는 보안 LDAP(LDAPS)와 함께 사용하도록 Insight를 구성하기 전에 회사 환경의 Active Directory 구성을 기록해 두십시오. Insight 설정은 조직의 LDAP 도메인 구성에 있는 설정과 일치해야 합니다. LDAP와 함께 사용하도록 Insight를 구성하기 전에 아래 개념을 검토하고 LDAP 도메인 관리자에게 해당 환경에서 사용할 수 있는 적절한 속성을 확인하십시오.

모든 보안 Active Directory(예: LDAPS) 사용자의 경우 인증서에 정의된 대로 AD 서버 이름을 정확히 사용해야 합니다. 보안 AD 로그인에 IP 주소를 사용할 수 없습니다.

를 사용하여 _server.keystore_and/or_server.trutstore_passwords"SecurityAdmin 을 클릭합니다"를 변경한 경우 LDAP 인증서를 가져오기 전에 _SANscreen_service를 다시 시작하십시오.

OnCommand Insight는 Microsoft Active Directory 서버 또는 Azure AD를 통해 LDAP 및 LDAPS를 지원합니다. 추가 LDAP 구현은 작동할 수 있지만 Insight에서 검증되지 않았습니다. 이 가이드의 절차에서는 Microsoft Active Directory 버전 2 또는 3 LDAP(Lightweight Directory Access Protocol)를 사용하고 있다고 가정합니다.

- 사용자 기본 이름 속성: *

LDAP 사용자 기본 이름 속성(userPrincipalName)은 Insight에서 사용자 이름 속성으로 사용하는 속성입니다. 사용자 주체 이름은 AD(Active Directory) 포리스트에서 전역적으로 고유하도록 보장되지만 많은 대규모 조직에서 사용자의 주 이름이 즉시 분명하지 않거나 알려지지 않을 수 있습니다. 조직에서 기본 사용자 이름에 사용자 기본 이름 속성 대신 을 사용할 수 있습니다.

다음은 User Principal Name 속성 필드에 대한 몇 가지 대체 값입니다.

- * sAMAccountName *

  이 사용자 속성은 기존 Windows 2000 NT 이전 사용자 이름입니다. 대부분의 사용자가 개인 Windows 시스템에 로그인하는 데 익숙합니다. 이는 AD 포리스트 전체에서 전체적으로 고유한 것으로 보장되지는 않습니다.

  sAMAccountName은 User Principal Name 속성에 대해 대/소문자를 구분합니다.

- 메일 *

  MS Exchange가 있는 AD 환경에서는 이 속성이 최종 사용자의 기본 이메일 주소입니다. 이는 해당 userPrincipalName 특성과 달리 AD 포리스트 전체에서 전역적으로 고유해야 하며 최종 사용자에게 익숙한 것이어야 합니다. 대부분의 비 MS Exchange 환경에는 메일 특성이 없습니다.

- * 조회 *

  LDAP 호출은 요청된 개체의 복사본이 없거나 더 정확하게는 클라이언트 응용 프로그램에 대한 도메인 컨트롤러의 표시 방식입니다. 실제로 존재하는 경우 해당 개체가 될 디렉터리 트리의 섹션을 보유하지 않고 클라이언트에 개체를 보관할 수 있는 위치를 제공합니다. 클라이언트는 도메인 컨트롤러에 대한 DNS 검색 기준으로 조회를 사용합니다. 가장 이상적인 방법은 항상 개체를 포함하는 도메인 컨트롤러를 참조하는 것입니다. 그러나 참조된 도메인 컨트롤러가 다른 조회를 생성할 수는 있지만 일반적으로 개체가 존재하지 않는다는 사실을 발견하고

클라이언트에 알리는 데 시간이 오래 걸리지는 않습니다.

sAMAccountName은 일반적으로 User Principal Name 보다 선호됩니다. sAMAccountName은 도메인에서 고유하지만(도메인 포리스트에서는 고유하지 않을 수 있음) 일반적으로 로그인에 사용하는 문자열 도메인 사용자입니다(예: *NetApp\username*). 고유 이름은 포리스트의 고유 이름이지만 일반적으로 사용자가 알 수 없습니다.

동일한 도메인의 Windows 시스템 부분에서 항상 명령 프롬프트를 열고 set 을 입력하여 적절한 도메인 이름(USERDOMAIN=)을 찾을 수 있습니다. 그러면 OCI 로그인 이름이 가 됩니다 `USERDOMAIN\sAMAccountName`.

도메인 이름 * mydomain.x.y.z.com * 에 를 사용합니다 `DC=x,DC=y,DC=z,DC=com` Insight의 Domain 필드

- 포트 *:

LDAP의 기본 포트는 389이고 LDAPS의 기본 포트는 636입니다

LDAPS의 일반 URL: `ldaps://<ldap_server_host_name>:636`

로그 위치:`\\<install directory>\SANscreen\wildfly\standalone\log\ldap.log`

기본적으로 Insight는 다음 필드에 표시된 값을 예상합니다. Active Directory 환경에서 이러한 변경 사항이 발생할 경우 Insight LDAP 구성에서 변경해야 합니다.

역할 속성
멤버
메일 속성입니다
메일
고유 이름 특성입니다
DistinguishedName입니다
불합격
를 따릅니다

그룹: *

OnCommand Insight 및 DWH 서버에서 서로 다른 액세스 역할을 가진 사용자를 인증하려면 Active Directory에서 그룹을 만들고 OnCommand Insight 및 DWH 서버에 해당 그룹 이름을 입력해야 합니다. 아래 그룹 이름은 예제일 뿐이며 Insight에서 LDAP에 대해 구성하는 이름은 Active Directory 환경에 대해 설정된 이름과 일치해야 합니다.

Insight Group	예
Insight 서버 관리자 그룹	insight.server.admins
Insight administrators 그룹	Insight.admins입니다
Insight 사용자 그룹	insight.users
Insight Guest 그룹	Insight.게스트
보고 관리자 그룹	Insight.report.admins입니다
보고 전문가 저자 그룹	insight.report.proauthors
보고 작성자 그룹	insight.report.business.authors
보고 소비자 그룹	Insight.report.business.consumer 를 참조하십시오
보고 받는 사람 그룹	Insight.report.수신자

LDAP를 사용하여 사용자 정의 구성

LDAP 서버에서 사용자 인증 및 승인을 위해 OnCommand Insight(OCI)를 구성하려면 OnCommand Insight 서버 관리자로 LDAP 서버에 정의되어 있어야 합니다.

시작하기 전에

LDAP 도메인에서 Insight에 대해 구성된 사용자 및 그룹 속성을 알아야 합니다.

모든 보안 Active Directory(예: LDAPS) 사용자의 경우 인증서에 정의된 대로 AD 서버 이름을 정확히 사용해야 합니다. 보안 AD 로그인에 IP 주소를 사용할 수 없습니다.

를 사용하여 _server.keystore_and/or_server.trutstore_passwords"SecurityAdmin 을 클릭합니다"를 변경한 경우 LDAP 인증서를 가져오기 전에 _SANscreen_service를 다시 시작하십시오.

이 작업에 대해

OnCommand Insight는 Microsoft Active Directory 서버를 통해 LDAP 및 LDAPS를 지원합니다. 추가 LDAP 구현은 작동할 수 있지만 Insight에서 검증되지 않았습니다. 이 절차에서는 Microsoft Active Directory 버전 2 또는 3 LDAP(Lightweight Directory Access Protocol)를 사용하고 있다고 가정합니다.

LDAP 사용자는 * Admin * > menu:Setup [Users](설정 [사용자]) 목록에 로컬로 정의된 사용자와 함께 표시됩니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 설정 * 을 클릭합니다.
3. 사용자 * 탭을 클릭합니다.
4. LDAP 섹션으로 스크롤합니다.
5. LDAP 사용자 인증 및 권한 부여를 허용하려면 * LDAP 활성화 * 를 클릭합니다.
6. 다음 필드에 내용을 입력합니다.

   ◦ `LDAP servers`:Insight는 쉼표로 구분된 LDAP URL 목록을 허용합니다. Insight는 LDAP 프로토콜의 유효성을 검사하지 않고 제공된 URL에 연결을 시도합니다.

   > LDAP 인증서를 가져오려면 * Certificates * 를 클릭하고 인증서 파일을 자동으로 가져오거나 수동으로 찾습니다.

   LDAP 서버를 식별하는 데 사용되는 IP 주소 또는 DNS 이름은 일반적으로 다음 형식으로 입력됩니다.

   ```
   ldap://<ldap-server-address>:port
   ```

   또는 기본 포트를 사용하는 경우:

   ```
   ldap://<ldap-server-address>
   ```

   + 이 필드에 여러 LDAP 서버를 입력할 때 각 항목에 올바른 포트 번호가 사용되는지 확인하십시오.

   ◦ `User name`: LDAP 서버에서 디렉터리 조회 쿼리에 대해 승인된 사용자의 자격 증명을 입력합니다.

   ◦ `Password`: 위 사용자의 암호를 입력합니다. LDAP 서버에서 이 암호를 확인하려면 * Validate * 를 클릭합니다.

7. 이 LDAP 사용자를 보다 정확하게 정의하려면 * 더 보기 * 를 클릭하고 나열된 속성의 필드를 채웁니다.

   이러한 설정은 LDAP 도메인에 구성된 속성과 일치해야 합니다. 이러한 필드에 입력할 값이 확실하지 않으면 Active Directory 관리자에게 문의하십시오.

   ◦ * Admins 그룹 *

   Insight Administrator 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 입니다 `insight.admins`.

   ◦ * 사용자 그룹 *

   Insight 사용자 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 입니다 `insight.users`.

   ◦ * 손님 그룹 *

   Insight 게스트 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 입니다 `insight.guests`.

◦ * 서버 관리자 그룹 *

Insight Server 관리자 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 입니다 `insight.server.admins`.

◦ * 시간 초과 *

시간 초과 전에 LDAP 서버의 응답을 기다리는 시간(밀리초)입니다. 기본값은 2,000이며, 모든 경우에 적절하며 수정할 수 없습니다.

◦ * 도메인 *

OnCommand Insight가 LDAP 사용자를 찾기 시작해야 하는 LDAP 노드입니다. 일반적으로 조직의 최상위 도메인입니다. 예를 들면 다음과 같습니다.

```
DC=<enterprise>,DC=com
```

◦ * 사용자 기본 이름 속성 *

LDAP 서버의 각 사용자를 식별하는 속성입니다. 기본값은 입니다 `userPrincipalName`이는 세계적으로 고유한 기능입니다. OnCommand Insight는 이 특성의 내용과 위에서 제공한 사용자 이름을 일치시킵니다.

◦ * 역할 속성 *

지정된 그룹 내에서 사용자의 맞춤을 식별하는 LDAP 속성입니다. 기본값은 입니다 `memberOf`.

◦ * 메일 속성 *

사용자의 이메일 주소를 식별하는 LDAP 속성입니다. 기본값은 입니다 `mail`. 이 기능은 OnCommand Insight에서 제공하는 보고서를 구독하려는 경우에 유용합니다. Insight는 각 사용자가 처음 로그인할 때 사용자의 이메일 주소를 선택하며, 그 후에는 이를 찾아보지 않습니다.

LDAP 서버에서 사용자의 이메일 주소가 변경되면 Insight에서 업데이트해야 합니다.

◦ * 고유 이름 특성 *

사용자의 고유 이름을 식별하는 LDAP 속성입니다. 기본값은 입니다 `distinguishedName`.

8. 저장 * 을 클릭합니다.