

Horizon 7 관리

2019년 3월 14일

VMware Horizon 7 7.8



vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

<https://docs.vmware.com/kr/>

VMware 웹 사이트에서는 최신 제품 업데이트도 제공합니다.

본 문서에 대한 의견이 있으시면 다음 주소로 피드백을 보내주십시오.

docfeedback@vmware.com

VMware, Inc.

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

VMware 코리아

서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화: +82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

목차

Horizon 7 관리 6

1 Horizon Administrator 사용 7

Horizon Administrator 및 Horizon 연결 서버 7

Horizon Administrator에 로그인 8

Horizon Administrator 인터페이스 사용 팁 9

Horizon Administrator에서 텍스트 표시 문제 해결 10

2 Horizon 연결 서버 구성 12

vCenter Server 및 View Composer 구성 12

Horizon 연결 서버 백업 26

클라이언트 세션 설정 구성 26

Horizon 연결 서버를 사용 또는 사용하지 않도록 설정 41

외부 URL 편집 42

고객 환경 개선 프로그램 참여 또는 철회 43

View LDAP 디렉토리 44

3 스마트 카드 인증 설정 46

스마트 카드를 사용하여 로그인 46

Horizon 연결 서버에서 스마트 카드 인증 구성 47

타사 솔루션에서 스마트 카드 인증 구성 53

스마트 카드 인증을 위한 Active Directory 준비 54

스마트 카드 인증 구성 확인 57

스마트 카드 인증서 해지 검사 사용 58

4 다른 유형의 사용자 인증 설정 63

2 요소 인증 사용 63

SAML 인증 사용 67

생체 인식 인증 구성 74

5 자격 증명을 요구하지 않고 사용자 인증 75

게시된 애플리케이션에 대해 인증되지 않은 액세스 제공 76

하이브리드 로그인에 대해 사용자 구성 82

Windows 기반 Horizon Client 에서 제공하는 현재 사용자로 로그인 기능 사용 83

모바일 및 Mac Horizon Client에서 자격 증명 저장 84

True SSO 설정 85

- 6 역할 기반 위임된 관리 구성 114**
 - 역할 및 권한 이해 114
 - 액세스 그룹을 사용하여 풀 및 팜 관리 위임 115
 - 사용 권한 이해 116
 - 관리자 관리 117
 - 사용 권한 관리 및 검토 119
 - 액세스 그룹 관리 및 검토 121
 - 사용자 지정 역할 관리 123
 - 미리 정의된 역할 및 권한 125
 - 일반 작업에 필요한 권한 129
 - 관리자 사용자 및 그룹의 모범 사례 133
- 7 Horizon Administrator 및 Active Directory에서 정책 구성 134**
 - Horizon Administrator에서 정책 설정 134
 - Horizon 7 그룹 정책 관리 템플릿 파일 사용 137
- 8 Horizon 7 구성 요소 유지 보수 144**
 - Horizon 7 구성 데이터 백업 및 복원 144
 - Horizon 7 구성 요소 모니터링 153
 - 시스템 상태 모니터링 154
 - Horizon 7 서비스 이해 154
 - 제품 라이선스 키 변경 157
 - 제품 라이선스 사용량 모니터링 157
 - Active Directory에서 일반 사용자 정보 업데이트 159
 - 다른 시스템으로 View Composer 마이그레이션 160
 - 연결 서버 인스턴스, 보안 서버 또는 View Composer의 인증서 업데이트 166
 - 고객 환경 향상 프로그램 167
- 9 Horizon Administrator에서 ThinApp 애플리케이션 관리 168**
 - ThinApp 애플리케이션을 위한 Horizon 7 요구 사항 168
 - 애플리케이션 패키지 캡처 및 저장 169
 - 시스템 및 데스크톱 풀에 ThinApp 애플리케이션 할당 173
 - Horizon Administrator에서 ThinApp 애플리케이션 유지 관리 180
 - Horizon Administrator에서 ThinApp 애플리케이션 모니터링 및 문제 해결 184
 - ThinApp 구성 예 188
- 10 키오스크 모드에서 클라이언트 설정 190**
 - 키오스크 모드에서 클라이언트 구성 190
- 11 Horizon 7 문제 해결 201**
 - Horizon Help Desk Tool 사용 201
 - VMware Logon Monitor 사용 212

VMware Horizon 성능 추적기 사용	217
시스템 상태 모니터링	221
Horizon 7 의 이벤트 모니터링	222
Horizon 7 의 진단 정보 수집	223
지원 요청 업데이트	227
보안 서버와 Horizon 연결 서버와의 연결 실패 문제 해결	228
Horizon 7 Server 인증서 해지 검사 문제 해결	229
스마트 카드 인증서 해지 검사 문제 해결	230
문제 해결 추가 정보	230

12 vdmadmin 명령 사용 231

vdmadmin 명령 사용	233
-A 옵션을 사용하여 Horizon Agent 로그인 구성	235
-A 옵션을 사용하여 IP 주소 재정의	238
-F 옵션을 사용하여 외부 보안 주체 업데이트	239
-H 옵션을 사용하여 상태 모니터 나열 및 표시	240
-I 옵션을 사용한 Horizon 7 작업 보고서 나열 및 표시	241
-i 옵션을 사용하여 Syslog 형식으로 Horizon 7 이벤트 로그 메시지 생성	242
-L 옵션을 사용하여 전용 시스템 할당	244
-M 옵션을 사용하여 시스템 정보 표시	245
-M 옵션을 사용하여 가상 시스템의 디스크 공간 회수	246
-N 옵션을 사용하여 도메인 필터 구성	247
도메인 필터 구성	250
-O 및 -P 옵션을 사용하여 권한 없는 사용자의 시스템 및 정책 표시	254
-Q 옵션을 사용하여 키오스크 모드에서 클라이언트 구성	256
-R 옵션을 사용하여 시스템의 첫 번째 사용자 표시	261
-S 옵션을 사용하여 연결 서버 인스턴스 또는 보안 서버의 항목 제거	261
-T 옵션을 사용하는 관리자에게 보조 자격 증명 제공	262
-U 옵션을 사용한 사용자 정보 표시	264
-V 옵션을 사용하여 가상 시스템 잠금 해제 또는 잠금	265
-X 옵션을 사용한 LDAP 항목 및 스키마 충돌 감지 및 해결	266

Horizon 7 관리

Horizon 7 관리에서는 Horizon 연결 서버 구성, 관리자 생성, 사용자 인증 설정, 정책 구성, Horizon Administrator에서 VMware ThinApp® 애플리케이션 관리 방법 등을 포함해 VMware Horizon 7®을 구성하고 관리하는 방법을 설명합니다. 이 문서에서는 Horizon 7 구성 요소를 유지 관리하고 문제를 해결하는 방법에 대해서도 설명합니다.

대상

이 정보는 VMware Horizon 7을 구성하고 관리하는 모든 사용자를 대상으로 합니다. 이 정보는 가상 시스템 기술과 데이터 센터 운영에 익숙하고 경험 많은 Windows 또는 Linux 시스템 관리자를 대상으로 작성되었습니다.

Horizon Administrator 사용

Horizon Administrator는 Horizon 연결 서버를 구성하고 원격 데스크톱 및 애플리케이션을 관리하는 웹 인터페이스입니다.

Horizon Administrator, cmdlet 및 vdmadmin을 사용하여 실행할 수 있는 작업을 비교하려면 Horizon 7 통합 문서를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [Horizon Administrator 및 Horizon 연결 서버](#)
- [Horizon Administrator에 로그인](#)
- [Horizon Administrator 인터페이스 사용 팁](#)
- [Horizon Administrator에서 텍스트 표시 문제 해결](#)

Horizon Administrator 및 Horizon 연결 서버

Horizon Administrator는 Horizon 7에 대한 웹 기반 관리 인터페이스를 제공합니다.

Horizon 연결 서버에는 복제 서버 또는 보안 서버로 작동하는 여러 인스턴스가 포함될 수 있습니다. Horizon 7 배포에 따라 각 연결 서버의 인스턴스가 있는 Horizon Administrator 인터페이스를 사용할 수 있습니다.

다음의 모범 사례를 활용하여 연결 서버에서 Horizon Administrator를 사용하십시오.

- 연결 서버의 호스트 이름 및 IP 주소를 사용하여 Horizon Administrator에 로그인합니다. Horizon Administrator 인터페이스를 사용하여 연결 서버와 모든 관련 보안 서버 또는 복제 서버를 관리합니다.
- 포드 환경에서는 모든 관리자가 동일한 연결 서버의 호스트 이름 및 IP 주소를 사용하여 Horizon Administrator에 로그인하는지 확인합니다. Horizon Administrator 웹 페이지에 액세스할 때는 로드 밸런서의 호스트 이름 및 IP 주소를 사용하지 마십시오.
- 사용 중인 연결 서버 포드를 식별하려면 Horizon Administrator 머릿글 및 웹 브라우저 탭에서 포드 이름을 확인하면 됩니다.

참고 보안 서버 대신 Unified Access Gateway 장치를 사용하는 경우에는 Unified Access Gateway REST API를 사용하여 Unified Access Gateway 장치를 관리해야 합니다. Unified Access Gateway의 이전 버전 이름은 Access Point입니다. 자세한 내용은 Unified Access Gateway 배포 및 구성의 내용을 참조하십시오.

Horizon Administrator에 로그인

초기 구성 작업을 수행하려면 Horizon Administrator에 로그인해야 합니다. 보안(TLS) 연결을 사용해 Horizon Administrator에 액세스합니다.

사전 요구 사항

- 전용 컴퓨터에 Horizon 연결 서버가 설치되어 있는지 확인하십시오.
- Horizon Administrator에서 지원하는 웹 브라우저를 사용하는지 확인하십시오. Horizon Administrator 요구 사항은 Horizon 7 설치 문서를 참조하십시오.

절차

- 1 웹 브라우저를 열고 다음 URL을 입력하십시오. `server`는 연결 서버 인스턴스의 호스트 이름입니다.

`https://server/admin`

참고 연결 서버 인스턴스에 액세스해야 하는데 호스트 이름을 확인할 수 없을 경우 IP 주소를 사용할 수 있습니다. 그러나 연결할 호스트가 연결 서버 인스턴스에 대해 구성된 TLS 인증서와 일치하지 않으면 액세스가 차단되거나 액세스 시 보안이 약화됩니다.

Horizon Administrator에 대한 액세스는 연결 서버 컴퓨터에 구성된 인증서의 유형에 따라 다릅니다.

연결 서버 호스트에서 웹 브라우저를 여는 경우 `https://localhost` 대신 `https://127.0.0.1`을 사용하여 연결합니다. 이렇게 하면 localhost 확인에서 잠재적인 DNS 공격이 방지되므로 보안이 강화됩니다.

옵션	설명
View 연결 서버에 대해 CA에서 서명한 인증서를 구성했습니다.	처음 연결할 때 웹 브라우저에 Horizon Administrator가 표시됩니다.
View 연결 서버에서 제공되는 기본 자체 서명 인증서가 구성됩니다.	처음 연결할 때 신뢰할 수 있는 인증서 기관에서 해당 주소와 연결된 보안 인증서를 발행하지 않았다는 내용의 경고 페이지가 웹 브라우저에 나타날 수 있습니다. 현재 TLS 인증서를 계속 사용하려면 무시 를 클릭합니다.

- 2 관리자 역할을 가진 계정을 사용하여 로그인합니다.

복제된 그룹에 독립 실행형 연결 서버 인스턴스 또는 첫 번째 연결 서버 인스턴스를 설치할 때 관리자 역할에 대한 초기 할당을 작성합니다. 기본적으로 연결 서버를 설치하는 데 사용하는 계정이 선택되지만 이 계정을 Administrators 로컬 그룹 또는 도메인 전역 그룹으로 변경할 수 있습니다.

Administrators 로컬 그룹을 선택한 경우 직접 또는 전역 그룹 구성원을 통해 이 그룹에 추가된 모든 도메인 사용자를 사용할 수 있습니다. 이 그룹에 추가된 로컬 사용자는 사용할 수 없습니다.

Horizon Administrator에 로그인한 후 **View 구성 > 관리자**를 통해 Administrators 역할을 가진 사용자 및 그룹의 목록을 변경할 수 있습니다.

Horizon Administrator 인터페이스 사용 팁

Horizon Administrator 사용자 인터페이스 기능을 사용하여 Horizon 페이지를 탐색하고 Horizon 개체를 찾아 필터링하고 정렬할 수 있습니다.

Horizon Administrator에는 일반 사용자 인터페이스 기능이 많습니다. 예를 들어, 각 페이지 왼쪽에 있는 탐색 창을 통해 다른 Horizon Administrator 페이지로 이동할 수 있습니다. 검색 필터를 사용하여 검색할 개체와 관련된 필터링 조건을 선택할 수 있습니다.

다음 표에서는 Horizon Administrator 사용에 도움을 줄 수 있는 몇 가지 추가 기능에 대해 설명합니다.

표 1-1. Horizon Administrator 탐색 및 디스플레이 기능

Horizon Administrator 기능	설명
Horizon Administrator 페이지 앞뒤 탐색	<p>브라우저의 뒤로 버튼을 클릭하여 이전에 표시된 Horizon Administrator 페이지로 이동합니다. 앞으로 단추를 클릭하여 현재 페이지로 돌아갑니다.</p> <p>Horizon Administrator 마법사 또는 대화 상자를 사용하는 동안 브라우저의 뒤로 버튼을 클릭하면 기본 Horizon Administrator 페이지로 돌아갑니다. 마법사 또는 대화 상자에 입력한 정보는 손실됩니다.</p> <p>View 5.1 이전 버전에서는 브라우저의 뒤로 및 앞으로 버튼을 사용하여 Horizon Administrator 내에서 이동할 수 없습니다. Horizon Administrator 창에 별도의 뒤로 및 앞으로 버튼이 탐색용으로 제공되었습니다. View 5.1 릴리스에서는 해당 버튼이 제거되었습니다.</p>
Horizon Administrator 페이지에 체크박스 설정	<p>브라우저에서 Horizon Administrator 페이지에 체크박스를 설정할 수 있습니다.</p>
여러 열 정렬	<p>여러 열 정렬을 사용하여 다양한 방법으로 Horizon 개체를 정렬할 수 있습니다. Horizon Administrator 테이블 첫 행의 머리글을 클릭하여 해당 머리글을 기반으로 알파벳 순서로 Horizon 개체를 정렬합니다.</p> <p>예를 들어, 리소스 > 시스템 페이지에서 데스크톱 풀을 클릭하여 포함하는 풀별로 데스크톱을 정렬할 수 있습니다.</p> <p>숫자 1은 머리글 옆에 나타나 기본 정렬 열을 표시합니다. 머리글을 다시 클릭하여 위 또는 아래쪽 화살표로 표시된 정렬 순서를 바꿀 수 있습니다.</p> <p>다른 항목별로 Horizon 개체를 정렬하려면 Ctrl 키를 누른 상태로 다른 머리글을 클릭합니다.</p> <p>예를 들어, 시스템 테이블에서 사용자를 클릭하여 데스크톱이 전용으로 할당된 사용자별로 두 번째 정렬을 수행할 수 있습니다. 숫자 2는 다른 머리글 옆에 나타납니다. 이 예에서 데스크톱은 각 풀 내 사용자 및 풀별로 정렬됩니다.</p> <p>계속 Ctrl+클릭하여 중요도 내림차순으로 테이블의 모든 열을 정렬할 수 있습니다.</p> <p>Ctrl+Shift를 누르고 클릭하여 정렬 항목 선택을 해제합니다.</p> <p>예를 들어, 특정 상태에 있으면서 특정 데이터스토어에 저장된 풀의 데스크톱을 표시할 수 있습니다. 리소스 > 시스템을 선택하고 데이터스토어 머리글을 클릭한 다음 Ctrl 키를 누른 상태로 상태 머리글을 클릭할 수 있습니다.</p>

표 1-1. Horizon Administrator 탐색 및 디스플레이 기능 (계속)

Horizon Administrator 기능	설명
테이블 열 사용자 지정	<p>선택한 열을 숨기고 첫 번째 열을 잠가서 Horizon Administrator 테이블 열의 표시를 사용자 지정할 수 있습니다. 이 기능을 통해 많은 열이 포함된 카탈로그 > 데스크톱 풀과 같은 큰 테이블의 표시를 제어할 수 있습니다.</p> <p>열 머리글을 마우스 오른쪽 버튼으로 클릭하면 표시되는 컨텍스트 메뉴를 통해 다음과 같은 작업을 수행할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 선택한 열을 숨깁니다. ■ 열을 사용자 지정합니다. 대화 상자에 테이블의 모든 열이 표시됩니다. 열을 선택하여 표시하거나 숨길 수 있습니다. ■ 첫 번째 열을 잠급니다. 이 옵션은 많은 열이 포함된 테이블에서 가로 방향으로 스크롤할 때 왼쪽 열이 표시된 상태로 유지되도록 합니다. 예를 들어, 카탈로그 > 데스크톱 풀 페이지에서 다른 데스크톱 특징을 보기 위해 가로 방향으로 스크롤할 때 데스크톱 ID가 표시된 상태로 유지됩니다.
Horizon 개체 선택 및 Horizon 개체 세부 정보 표시	<p>Horizon 개체를 나열하는 Horizon Administrator에서 개체를 선택하거나 개체 세부 정보를 표시할 수 있습니다.</p> <ul style="list-style-type: none"> ■ 개체를 선택하려면 테이블에서 개체의 행 어디든지 클릭합니다. 페이지 상단에서 개체를 관리하는 메뉴 및 명령이 활성화됩니다. ■ 개체 세부 정보를 표시하려면 개체 행의 왼쪽 셀을 두 번 클릭합니다. 새 페이지는 개체의 세부 정보를 표시합니다. <p>예를 들어, 카탈로그 > 데스크톱 풀 페이지의 개별 풀 행에서 어디든지 클릭하여 풀에 영향을 주는 명령을 활성화합니다.</p> <p>왼쪽 열에서 ID 셀을 두 번 클릭하여 풀에 대한 세부 정보가 포함된 새 페이지를 표시합니다.</p>
세부 정보를 보기 위해 대화 상자 확장	<p>Horizon Administrator 대화 상자를 확장하여 테이블 열의 데스크톱 이름 및 사용자 이름과 같은 세부 정보를 볼 수 있습니다.</p> <p>대화 상자를 확장하려면 대화 상자의 오른쪽 하단 모서리에 있는 점 위에 마우스를 놓고 모서리를 끕니다.</p>
Horizon 개체의 컨텍스트 메뉴 표시	<p>Horizon Administrator 테이블에서 Horizon 개체를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 표시할 수 있습니다. 컨텍스트 메뉴를 사용하면 선택한 Horizon 개체에 대해 작동하는 명령에 액세스할 수 있습니다.</p> <p>예를 들어, 카탈로그 > 데스크톱 풀 페이지에서 데스크톱 풀을 마우스 오른쪽 버튼으로 클릭하여 추가, 편집, 삭제, 프로비저닝 사용 안 함(또는 사용) 등의 명령을 표시할 수 있습니다.</p>

Horizon Administrator에서 텍스트 표시 문제 해결

Linux, UNIX 또는 Mac OS와 같은 비 Windows 운영 체제에서 웹 브라우저를 실행할 경우 Horizon Administrator의 텍스트가 올바르게 표시되지 않습니다.

문제

Horizon Administrator 인터페이스의 텍스트가 제대로 표시되지 않습니다. 예를 들어, 단어 중간에 공백이 발생합니다.

원인

Horizon Administrator에는 Microsoft 특정 글꼴이 필요합니다.

해결책

컴퓨터에 Microsoft 특정 글꼴을 설치하십시오.

현재 Microsoft 웹 사이트에서는 Microsoft 글꼴을 배포하지 않지만 독립 웹 사이트에서 다운로드 할 수 있습니다.

Horizon 연결 서버 구성

Horizon 연결 서버를 설치하고 초기 구성을 수행한 후에 Horizon 7 배포에 vCenter Server 인스턴스와 View Composer 서비스를 추가하고 관리자 업무를 위임할 역할을 설정하며 구성 데이터 백업 작업을 예약할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- vCenter Server 및 View Composer 구성
- Horizon 연결 서버 백업
- 클라이언트 세션 설정 구성
- Horizon 연결 서버를 사용 또는 사용하지 않도록 설정
- 외부 URL 편집
- 고객 환경 개선 프로그램 참여 또는 철회
- View LDAP 디렉토리

vCenter Server 및 View Composer 구성

가상 시스템을 원격 데스크톱으로 사용하려면 vCenter Server와 통신하도록 View를 구성해야 합니다. 연결된 클론 데스크톱 풀을 생성하고 관리하려면 Horizon Administrator에서 View Composer 설정을 구성해야 합니다.

Horizon 7에 대해 스토리지 설정을 구성할 수도 있습니다. ESXi 호스트가 연결된 클론 가상 시스템의 디스크 공간을 회수하도록 허용할 수 있습니다. ESXi 호스트가 가상 시스템 데이터를 캐시하도록 허용하려면 vCenter Server의 View Storage Accelerator를 사용하도록 설정해야 합니다.

View Composer AD 작업을 위한 사용자 계정 생성

View Composer를 사용하는 경우 View Composer가 Active Directory에서 특정 작업을 수행하도록 허용하는 Active Directory의 사용자 계정을 생성해야 합니다. View Composer에서는 연결된 클론 가상 시스템을 Active Directory 도메인에 가입시키기 위해 이 계정을 필요로 합니다.

보안 상의 이유로 View Composer에서 사용할 사용자 계정을 별도로 생성해야 합니다. 별도 계정을 생성해 다른 용도로 정의된 추가 권한을 가지고 있지 않도록 보장할 수 있습니다. 특정 Active Directory 컨테이너에서 컴퓨터 개체를 생성 또는 제거하는데 필요한 최소 권한을 계정에 부여할 수 있습니다. 예를 들어 View Composer 계정에는 도메인 관리자 권한이 필요하지 않습니다.

절차

- 1 Active Directory에서 연결 서버 호스트와 동일한 도메인 또는 신뢰할 수 있는 도메인에서 사용자 계정을 생성하십시오.
- 2 연결된 클론 컴퓨터 계정을 생성하거나 연결된 클론 컴퓨터 계정을 이동한 Active Directory 컨테이너 계정에 **컴퓨터 개체 생성**, **컴퓨터 개체 삭제** 및 **모든 속성 쓰기** 사용 권한을 추가하십시오.

다음 목록은 기본으로 할당된 사용 권한을 포함해 사용자 계정에 필요한 모든 사용 권한을 보여줍니다.

- 목록 내용
- 모든 속성 읽기
- 모든 속성 쓰기
- 사용 권한 읽기
- 암호 재설정
- 컴퓨터 개체 생성
- 컴퓨터 개체 삭제

참고 데스크톱 풀에 대해 **기존 컴퓨터 계정의 재사용 허용** 설정을 선택하는 경우 보다 적은 사용 권한이 필요합니다. 다음과 같은 사용 권한이 사용자 계정에 할당되어 있는지 확인하십시오.

- 목록 내용
- 모든 속성 읽기
- 사용 권한 읽기
- 암호 재설정

- 3 Active Directory 컨테이너 및 컨테이너의 모든 하위 개체에 사용자 계정의 사용 권한을 적용했는지 확인하십시오.

다음에 수행할 작업

vCenter Server 추가 마법사에서 View Composer 도메인을 구성하거나 연결된 클론 데스크톱 풀을 구성 및 배포할 때 Horizon Administrator에서 계정을 지정하십시오.

Horizon 7 에 vCenter Server 인스턴스 추가

Horizon 7 배포에서 vCenter Server 인스턴스에 연결하도록 Horizon 7을 구성해야 합니다.

vCenter Server는 Horizon 7이 데스크톱 풀에서 사용하는 가상 시스템을 생성하고 관리합니다.

Linked Mode 그룹에서 vCenter Server 인스턴스를 실행하려면 각 vCenter Server 인스턴스를 Horizon 7에 따로 추가해야 합니다.

Horizon 7는 보안 채널(SSL)을 사용해 vCenter Server 인스턴스에 연결합니다.

사전 요구 사항

- 연결 서버 제품 라이선스 키를 설치하십시오.
- vCenter Server 사용자가 vCenter Server에서 Horizon 7를 지원하는 데 필요한 작업을 수행할 수 있는 사용 권한을 가지도록 준비하십시오. View Composer를 사용하려면 사용자에게 추가 권한을 부여해야 합니다.

Horizon 7에 대해 vCenter Server 사용자를 구성하는 방법에 대한 자세한 내용은 Horizon 7 설치 문서를 참조하십시오.

- TLS/SSL 서버 인증서가 vCenter Server 호스트에 설치되어 있는지 확인하십시오. 운영 환경에는 신뢰할 수 있는 인증 기관(CA)에서 서명한 유효한 인증서를 설치하십시오.

테스트 환경에서는 vCenter Server에 설치된 기본 인증서를 사용할 수 있지만 vCenter Server를 Horizon 7에 추가할 때 인증서 지문을 허용해야 합니다.

- 복제된 그룹의 모든 연결 서버 인스턴스가 vCenter Server 호스트에 설치된 서버 인증서의 루트 CA 인증서를 신뢰하는지 확인하십시오. 루트 CA 인증서가 연결 서버 호스트의 Windows 로컬 컴퓨터 인증서 저장소에 위치한 **신뢰할 수 있는 루트 인증 기관 > 인증서** 폴더에 있는지 확인하십시오. 없는 경우 루트 CA 인증서를 Windows 로컬 컴퓨터 인증서 저장소로 가져오십시오.

자세한 내용은 Horizon 7 설치 문서의 "Windows 인증서 저장소에 루트 인증서 및 중간 인증서 가져오기"를 참조하십시오.

- vCenter Server 인스턴스에 ESXi 호스트가 포함되어 있는지 확인하십시오. vCenter Server 인스턴스에 호스트가 구성되어 있지 않은 경우 인스턴스를 Horizon 7에 추가할 수 없습니다.
- vSphere 5.5 이후 릴리스로 업그레이드하는 경우 vCenter Server 사용자로 사용하는 도메인 관리자 계정에 vCenter Server 로컬 사용자가 vCenter Server로 로그인할 사용 권한이 명시적으로 할당되어 있는지 확인하십시오.
- Horizon 7을 FIPS 모드에서 사용하려는 경우에는 vCenter Server 6.0 이상 및 ESXi 6.0 이상 호스트가 있는지 확인하십시오.

자세한 내용은 Horizon 7 설치 문서의 "FIPS 모드에서 Horizon 7 설치"를 참조하십시오.

- vCenter Server와 View Composer의 최대 작업 수 제한을 결정하는 설정을 숙지하십시오. 자세한 내용은 [vCenter Server 및 View Composer의 동시 작업 수 제한](#) 및 [동시 전원 작업 수를 설정하여 원격 데스크톱 로그인 스톱 지원](#)의 내용을 참조하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 **vCenter Server** 탭에서 **추가**를 클릭합니다.

- 3 vCenter Server 설정 **서버 주소** 텍스트 상자에 vCenter Server 인스턴스의 FQDN(정규화된 도메인 이름)을 입력합니다.

FQDN에는 호스트 이름과 도메인 이름이 포함되어 있습니다. 예를 들어 FQDN

*myserverhost.companydomain.com*에서 *myserverhost*는 호스트 이름이고 *companydomain.com*은 도메인입니다.

참고 DNS 이름 또는 URL을 사용해 서버를 입력하면 Horizon 7에서 DNS 조회를 통해 이전에 관리자가 IP 주소를 사용하여 Horizon 7에 이 서버를 추가했는지 여부를 확인하지 않습니다. DNS 이름과 IP 주소를 모두 사용해 vCenter Server를 추가하면 충돌이 발생합니다.

- 4 vCenter Server 사용자 이름을 입력하십시오.

예: `domainWuser` 또는 `user@domain.com`

- 5 vCenter Server 사용자 암호를 입력하십시오.

- 6 (선택 사항) 이 vCenter Server 인스턴스에 대한 설명을 입력하십시오.

- 7 TCP 포트 번호를 입력하십시오.

기본 포트는 443입니다.

- 8 고급 설정에서 vCenter Server 및 View Composer 작업의 동시 작업 수 제한을 설정합니다.

- 9 다음을 클릭하여 View Composer 설정 페이지를 표시합니다.

다음에 수행할 작업

View Composer 설정을 구성합니다.

- vCenter Server 인스턴스가 서명된 SSL 인증서로 구성되고 연결 서버가 루트 인증서를 신뢰하면 vCenter Server 추가 마법사에 View Composer 설정 페이지가 표시됩니다.
- vCenter Server 인스턴스가 기본 인증서로 구성된 경우 먼저 기존 인증서의 지문을 허용할지 결정해야 합니다. [기본 TLS 인증서의 지문 허용](#)의 내용을 참조하십시오.

Horizon 7가 여러 vCenter Server 인스턴스를 사용하는 경우 이 절차를 반복해 다른 vCenter Server 인스턴스를 추가하십시오.

View Composer 설정 구성

View Composer를 사용하려면 Horizon 7가 VMware Horizon View Composer 서비스에 연결할 수 있도록 설정을 구성해야 합니다. View Composer는 내장된 별도의 호스트 또는 vCenter Server와 동일한 호스트에 설치할 수 있습니다.

각 VMware Horizon View Composer 서비스와 vCenter Server 인스턴스가 일대일로 매핑되어 있어야 합니다. View Composer 서비스는 vCenter Server 인스턴스 하나와만 작동할 수 있습니다. vCenter Server 인스턴스는 VMware Horizon View Composer 서비스 하나와만 연결될 수 있습니다.

처음 Horizon 7를 배포한 후 VMware Horizon View Composer 서비스를 새 호스트로 마이그레이션하여 Horizon 7 배포 확장 또는 변경을 지원할 수 있습니다. Horizon Administrator에서 초기 View Composer 설정을 편집할 수 있지만 마이그레이션이 성공하도록 하려면 추가 단계를 수행해야 합니다. [다른 시스템으로 View Composer 마이그레이션](#)의 내용을 참조하십시오.

사전 요구 사항

- 연결된 클론을 포함하는 Active Directory 도메인에서 가상 시스템을 추가 및 제거할 수 있는 사용 권한을 가진 사용자를 Active Directory에 생성했는지 확인하십시오. [View Composer AD 작업을 위한 사용자 계정 생성](#)의 내용을 참조하십시오.
- vCenter Server에 연결하도록 Horizon 7을 구성했는지 확인합니다. 그러려면 vCenter Server 추가 마법사의 vCenter Server 정보 페이지를 작성해야 합니다. [Horizon 7에 vCenter Server 인스턴스 추가](#)의 내용을 참조하십시오.
- 이 VMware Horizon View Composer 서비스가 아직 다른 vCenter Server 인스턴스에 연결하도록 구성되어 있지 않은지 확인합니다.

절차

- 1 Horizon Administrator에서 vCenter Server 추가 마법사의 vCenter Server 정보 페이지를 작성하십시오.

a **View 구성 > 서버**를 선택합니다.

b **vCenter Server** 탭에서 **추가**를 클릭하고 vCenter Server 설정을 제공합니다.

- 2 View Composer를 사용하지 않으려면 View Composer 설정 페이지에서 **View Composer 사용 안 함**을 선택하십시오.

View Composer 사용 안 함을 선택하면 다른 View Composer 설정이 비활성화됩니다. 다음을 클릭하면 vCenter Server 추가 마법사에 스토리지 설정 페이지가 표시됩니다. View Composer 도메인 페이지는 표시되지 않습니다.

- 3 View Composer를 사용할 경우 View Composer 호스트의 위치를 선택하십시오.

옵션	설명
View Composer는 vCenter Server와 동일한 호스트에 설치됩니다.	<ol style="list-style-type: none"> a vCenter Server와 함께 설치된 View Composer를 선택합니다. b 포트 번호가 vCenter Server에 VMware Horizon View Composer 서비스를 설치할 때 지정한 포트와 동일한지 확인합니다. 기본 포트 번호는 18443입니다.
View Composer는 내장된 별도의 호스트에 설치됩니다.	<ol style="list-style-type: none"> a 독립 실행형 View Composer Server를 선택합니다. b View Composer Server 주소 텍스트 상자에서 View Composer 호스트의 FQDN(정규화된 도메인 이름)을 입력합니다. c View Composer 사용자 이름을 입력합니다. 예: domain.com\user 또는 user@domain.com d View Composer 사용자 암호를 입력합니다. e 포트 번호가 VMware Horizon View Composer 서비스를 설치할 때 지정한 포트와 동일한지 확인합니다. 기본 포트 번호는 18443입니다.

- 4 다음을 클릭하여 View Composer 도메인 페이지를 표시합니다.

다음에 수행할 작업

View Composer 도메인을 구성합니다.

- View Composer 인스턴스가 서명된 TLS 인증서로 구성되고 연결 서버가 루트 인증서를 신뢰하면 vCenter Server 추가 마법사에 View Composer 도메인 페이지가 표시됩니다.
- View Composer 인스턴스가 기본 인증서로 구성된 경우 먼저 기존 인증서의 지문을 허용할지 결정해야 합니다. [기본 TLS 인증서의 지문 허용](#)의 내용을 참조하십시오.

View Composer 도메인 구성

View Composer가 연결된 클론 데스크톱을 배포할 Active Directory 도메인을 구성해야 합니다. View Composer에 대해 여러 도메인을 구성할 수 있습니다. 먼저 vCenter Server와 View Composer 설정을 View에 추가한 후 Horizon Administrator에서 vCenter Server 인스턴스를 편집하여 추가 View Composer 도메인을 추가할 수 있습니다.

사전 요구 사항

- Active Directory 관리자가 AD 작업에 대한 View Composer 사용자를 생성해야 합니다. 이 도메인 사용자는 연결된 클론이 포함된 Active Directory 도메인에서 가상 시스템을 추가 및 제거할 수 있는 사용 권한이 있어야 합니다. 이 사용자에게 필요한 사용 권한에 대한 자세한 내용은 [View Composer AD 작업을 위한 사용자 계정 생성](#)을 참조하십시오.
- Horizon Administrator에서 vCenter Server 추가 마법사의 vCenter Server 정보 및 View Composer 설정 페이지를 완료했는지 확인합니다.

절차

- 1 View Composer 도메인 페이지에서 **추가**를 클릭하여 AD 작업 계정 정보에 대한 View Composer 사용자를 추가하십시오.
- 2 Active Directory 도메인의 도메인 이름을 입력하십시오.
예: domain.com
- 3 View Composer 사용자의 도메인 이름을 포함한 도메인 사용자 이름을 입력하십시오.
예: domain.comWadmin
- 4 계정 암호를 입력하십시오.
- 5 **확인**을 클릭합니다.
- 6 연결된 클론 풀을 배포한 다른 Active Directory 도메인에 권한을 가진 도메인 사용자 계정을 추가하려면 앞의 단계를 반복하십시오.
- 7 **다음**을 클릭하여 스토리지 설정 페이지를 표시합니다.

다음에 수행할 작업

가상 시스템 디스크 공간 재사용을 사용하도록 설정하고 Horizon 7에 대해 View Storage Accelerator를 구성합니다.

vSphere가 연결된 클론 가상 시스템의 디스크 공간을 회수할 수 있도록 허용

vSphere 5.1 이상에서는 Horizon 7의 디스크 공간 회수 기능을 사용하도록 설정할 수 있습니다.

vSphere 5.1에서 시작하면 Horizon 7이 ESXi 호스트에서 연결된 클론의 사용되지 않은 디스크 공간을 재사용하여 연결된 클론에 필요한 총 스토리지 공간을 줄일 수 있는 효율적인 디스크 형식으로 연결된 클론 가상 시스템을 생성합니다.

사용자가 연결된 클론 데스크톱과 상호 작용하므로 클론의 OS 디스크가 확장되어 결국 거의 전체 클론 데스크톱과 비슷한 양의 디스크 공간을 사용할 수 있습니다. 디스크 공간 재사용을 사용하면 연결된 클론을 새로 고치거나 재구성할 필요 없이 OS 디스크의 크기를 줄일 수 있습니다. 가상 시스템의 전원이 켜져 있고 사용자가 원격 데스크톱과 상호 작용하고 있는 동안 공간을 재사용할 수 있습니다.

디스크 공간 재사용은 로그오프 시 새로 고침과 같은 스토리지 절약 전략을 활용할 수 없는 배포에 특히 유용합니다. 예를 들어, 전용 원격 데스크톱에 사용자 애플리케이션을 설치하는 지식 작업자는 원격 데스크톱을 새로 고치거나 재구성할 경우 개인 애플리케이션을 잃을 수 있습니다. 디스크 공간 재사용 기능을 사용하면 Horizon 7가 처음 프로비저닝될 때 시작하는 줄어든 크기에 가깝게 연결된 클론을 유지할 수 있습니다.

이 기능에는 공간 효율적인 디스크 형식 및 공간 재사용 작업의 두 가지 구성 요소가 있습니다.

vSphere 5.1 이상의 환경에서 상위 가상 시스템의 가상 하드웨어 버전이 9 이상인 경우 Horizon 7가 공간 재사용 작업의 설정 여부에 관계없이 공간 효율적인 OS 디스크 형식의 연결된 클론을 생성합니다.

공간 회수 작업을 사용하도록 설정하려면 Horizon Administrator를 사용해 vCenter Server에 대해 공간 재사용을 사용하도록 설정하고 개별 데스크톱 풀의 VM 디스크 공간을 회수해야 합니다.

vCenter Server의 공간 재사용 설정은 vCenter Server 인스턴스에 의해 관리되는 모든 데스크톱 풀에서 이 기능을 사용하지 않도록 설정할 수 있는 옵션을 제공합니다. vCenter Server에 대해 이 기능을 사용하지 않도록 설정하면 데스크톱 풀 수준에서 설정이 재정의됩니다.

공간 재사용 기능에 다음과 같은 지침이 적용됩니다.

- 연결된 클론의 공간 효율적인 OS 디스크에서만 작동합니다.
- View Composer 영구 디스크에는 영향을 주지 않습니다.
- vSphere 5.1 이상과 가상 하드웨어 버전 9 이상인 가상 시스템에서만 작동합니다.
- 전체 클론 데스크톱에서는 작동하지 않습니다.
- SCSI 컨트롤러가 있는 가상 시스템에서 작동합니다. IDE 컨트롤러는 지원되지 않습니다.

기본 NFS 스냅샷 기술(VAAI)은 공간 효율적인 디스크를 사용하는 가상 시스템이 포함된 풀에서는 지원되지 않습니다.

사전 요구 사항

- vCenter Server 및 ESXi 호스트(클러스터의 모든 ESXi 호스트 포함) 버전이 ESXi 5.1 다운로드 패치 ESXi510-201212001 이상이 적용된 5.1인지 확인합니다.

절차

- 1 Horizon Administrator에서 스토리지 설정 페이지 앞에 나오는 vCenter Server 추가 마법사 페이지를 완료합니다.
 - a **View 구성 > 서버**를 선택합니다.
 - b **vCenter Server** 탭에서 **추가**를 클릭합니다.
 - c vCenter Server 정보, View Composer 설정 및 View Composer 도메인 페이지를 완료합니다.
- 2 스토리지 설정 페이지에서 **공간 재사용을 사용하도록 설정**이 선택되었는지 확인합니다.

Horizon 7 5.2 이상을 새로 설치할 경우 공간 재사용이 기본적으로 선택됩니다. Horizon 7 5.1 또는 이전 릴리스에서 Horizon 7 5.2 이상으로 업그레이드할 경우 **공간 재사용을 사용하도록 설정**을 선택해야 합니다.

다음에 수행할 작업

스토리지 설정 페이지에서 View Storage Accelerator를 구성합니다.

Horizon 7에서 디스크 공간 재사용 구성을 완료하려면 데스크톱 풀에 대해 공간 재사용을 설정하십시오.

vCenter Server의 View Storage Accelerator 구성

vSphere 5.1 이상 버전의 경우, ESXi 호스트를 구성하여 가상 시스템 디스크 데이터를 캐시할 수 있습니다. View Storage Accelerator라는 이 기능은 ESXi 호스트의 CBRC(Content Based Read Cache) 기능을 사용합니다. View Storage Accelerator는 여러 가상 시스템이 한꺼번에 시작하거나 바이러스 백신 스캔을 실행할 때 발생할 수 있는 I/O 스톱 중 Horizon 7 성능을 향상시킵니다. 이 기능은 관리자 또는 사용자가 애플리케이션이나 데이터를 자주 로드하는 경우에도 유용합니다. 스토리지 시스템에서 전체 OS 또는 애플리케이션을 반복해서 읽는 대신, 호스트는 캐시에서 공통 데이터 블록을 읽을 수 있습니다.

부트 스톱 중 IOPS 수가 감소하면 View Storage Accelerator가 스토리지 어레이의 요구를 줄여 주고, 따라서 Horizon 7 배포를 지원하는 스토리지 I/O 대역폭을 덜 사용하게 됩니다.

이 절차에 설명된 대로 Horizon Administrator의 vCenter Server 마법사에서 View Storage Accelerator 설정을 선택하여 ESXi 호스트에서 캐싱을 사용하도록 설정합니다.

View Storage Accelerator가 개별 데스크톱 풀에 대해서도 구성되어 있는지 확인하십시오. 데스크톱 풀에서 작동하도록 하려면 View Storage Accelerator가 vCenter Server와 개별 데스크톱 풀에 사용하도록 설정되어 있어야 합니다.

View Storage Accelerator는 기본적으로 데스크톱 풀에 대해 사용하도록 설정되어 있습니다. 이 기능은 풀을 생성하거나 편집할 때 사용하거나 사용하지 않도록 설정할 수 있습니다. 가장 좋은 접근 방식은 처음 데스크톱 풀을 생성할 때 이 기능을 사용하도록 설정하는 것입니다. 기존 풀을 편집하여 이 기능을 사용하도록 설정하는 경우 연결된 클론이 프로비저닝되기 전에 새 복제본과 다이제스트 디스크를 생성해야 합니다. 새 스냅샷에 풀을 재구성하거나 새 데이터스토어로 풀을 재조정하여 새 복제본을 생성할 수 있습니다. 다이제스트 파일은 전원이 꺼질 때 데스크톱 풀의 가상 시스템에 대해서만 구성될 수 있습니다.

연결된 클론이 포함된 데스크톱 풀과 전체 가상 시스템이 포함된 풀에서 View Storage Accelerator를 사용하도록 설정할 수 있습니다.

기본 NFS 스냅샷 기술(VAAI)은 View Storage Accelerator에 대해 사용하도록 설정된 풀에서 지원되지 않습니다.

View Storage Accelerator는 이제 Horizon 7 복제본 계층화를 사용하는 구성에서 작동할 수 있으며 이 구성에서는 복제본이 연결된 클론이 아닌 개별 데이터스토어에 저장됩니다. View Storage Accelerator와 Horizon 7 복제본 계층화를 함께 사용할 경우 얻을 수 있는 성능 이점은 그리 크지 않지만 별도의 데이터스토어에 복제본을 저장함으로써 특정한 용량 관련 이점을 얻을 수 있습니다. 따라서 이 조합이 테스트 및 지원됩니다.

중요 이 기능을 사용하고자 하며 일부 ESXi 호스트를 공유하는 여러 개의 Horizon 7 포드를 사용하는 경우에는 공유 ESXi 호스트에 있는 모든 풀에 대해 Horizon Storage Accelerator 기능을 사용하도록 설정해야 합니다. 여러 개의 포드에서 설정에 일관성이 없는 경우에는 공유 ESXi 호스트의 가상 시스템에 불안정성이 발생할 수 있습니다.

사전 요구 사항

- vCenter Server 및 ESXi 호스트 버전이 5.1 이상인지 확인하십시오.
ESXi 클러스터에서 모든 호스트의 버전이 5.1 이상인지 확인하십시오.
- vCenter Server에서 vCenter Server 사용자에게 **호스트 > 구성 > 고급 설정** 권한이 할당되었는지 확인합니다.
Horizon 7 설치 문서에서 vCenter Server 사용자에게 필요한 Horizon 7 및 View Composer 권한에 대해 설명하는 항목을 참조하십시오.

절차

- 1 Horizon Administrator에서 스토리지 설정 페이지 앞에 나오는 vCenter Server 추가 마법사 페이지를 완료합니다.
 - a **View 구성 > 서버**를 선택합니다.
 - b **vCenter Server** 탭에서 **추가**를 클릭합니다.
 - c vCenter Server 정보, View Composer 설정 및 View Composer 도메인 페이지를 완료합니다.
- 2 스토리지 설정 페이지에서 **View Storage Accelerator 사용** 확인란이 선택되었는지 확인합니다.
이 확인란은 기본적으로 선택되어 있습니다.
- 3 기본 호스트 캐시 크기를 지정합니다.
기본 캐시 크기는 이 vCenter Server 인스턴스에서 관리하는 모든 ESXi 호스트에 적용됩니다.
기본값은 1,024MB입니다. 캐시 크기는 100MB와 2,048MB 사이여야 합니다.

- 4 개별 ESXi 호스트에 다른 캐시 크기를 지정하려면 ESXi 호스트를 선택하고 **캐시 크기 편집**을 클릭하십시오.
 - a 호스트 캐시 대화 상자에서 **기본 호스트 캐시 크기 재정의**를 선택합니다.
 - b 100MB와 2,048MB 사이의 **호스트 캐시 크기**를 입력하고 **확인**을 클릭합니다.
- 5 스토리지 설정 페이지에서 **다음**을 클릭합니다.
- 6 **마침**을 클릭하여 vCenter Server, View Composer 및 스토리지 설정을 Horizon 7에 추가합니다.

다음에 수행할 작업

클라이언트 세션 및 연결을 위한 설정을 구성합니다. [클라이언트 세션 설정 구성](#)를 참조하십시오.

Horizon 7에서 View Storage Accelerator 설정을 완료하려면 데스크톱 풀에 대해 View Storage Accelerator를 구성하십시오. Horizon 7에서 가상 데스크톱 설정 문서에서 “데스크톱 풀의 View Storage Accelerator 구성”을 참조하십시오.

vCenter Server 및 View Composer의 동시 작업 수 제한

vCenter Server를 Horizon 7에 추가하거나 vCenter Server 설정을 편집할 때 vCenter Server 및 View Composer에서 수행되는 최대 동시 작업 수를 설정하는 몇 가지 옵션을 구성할 수 있습니다.

이러한 옵션은 vCenter Server 정보 페이지의 고급 설정 패널에서 구성합니다.

표 2-1. vCenter Server 및 View Composer의 동시 작업 수 제한

설정	설명
최대 동시 vCenter 프로비저닝 작업 수	<p>연결 서버가 이 vCenter Server 인스턴스에서 전체 가상 시스템을 프로비저닝 및 삭제할 수 있는 최대 동시 요청 수를 결정합니다.</p> <p>기본값은 20입니다.</p> <p>이 설정은 전체 가상 시스템에만 적용됩니다.</p>
최대 동시 전원 작업 수	<p>이 vCenter Server 인스턴스의 연결 서버가 관리하는 가상 시스템에 대해 수행할 수 있는 최대 동시 전원 작업 수(시작, 종료, 일시 중단 등)를 결정합니다.</p> <p>기본값은 50입니다.</p> <p>이 설정의 값을 계산하는 방법에 대한 지침은 동시 전원 작업 수를 설정하여 원격 데스크톱 로그인 스톱 지원을 참조하십시오.</p> <p>이 설정은 전체 가상 시스템 및 연결된 클론에 적용됩니다.</p>

표 2-1. vCenter Server 및 View Composer의 동시 작업 수 제한 (계속)

설정	설명
최대 동시 View Composer 유지 관리 작업 수	<p>이 View Composer 인스턴스에서 관리하는 연결된 클론에 대해 수행할 수 있는 최대 동시 View Composer 새로 고침, 재구성 및 재조정 작업 수를 결정합니다.</p> <p>기본값은 12입니다.</p> <p>유지 관리 작업을 시작하려면 먼저 활성 세션이 있는 원격 데스크톱을 로그오프해야 합니다. 유지 관리 작업이 시작되는 즉시 사용자를 강제로 로그오프하는 경우 원격 데스크톱에서 로그오프가 필요한 최대 동시 작업 수는 구성된 값의 절반이 됩니다. 예를 들어, 이 설정을 24로 구성하고 강제로 사용자를 로그오프하는 경우 원격 데스크톱에서 로그오프가 필요한 최대 동시 작업 수는 12가 됩니다.</p> <p>이 설정은 연결된 클론에만 적용됩니다.</p>
최대 동시 View Composer 프로비저닝 작업 수	<p>이 View Composer 인스턴스에서 관리하는 연결된 클론에 대해 수행할 수 있는 최대 동시 생성 및 삭제 작업 수를 결정합니다.</p> <p>기본값은 8입니다.</p> <p>이 설정은 연결된 클론에만 적용됩니다.</p>

동시 전원 작업 수를 설정하여 원격 데스크톱 로그인 스톱 지원

최대 동시 전원 작업 수 설정은 vCenter Server 인스턴스의 원격 데스크톱 가상 시스템에서 발생할 수 있는 최대 동시 전원 작업 수를 제어합니다. 이 제한은 기본적으로 50으로 설정됩니다. 이 값을 변경하여 많은 사용자가 동시에 데스크톱에 로그인할 경우 피크 전원 작업 수를 지원할 수 있습니다.

시험 단계를 수행하여 이 설정의 올바른 값을 결정하는 것이 가장 좋습니다. 계획 지침은 Horizon 7 아키텍처 계획 문서의 "아키텍처 설계 요소 및 계획 지침"을 참조하십시오.

필요한 동시 전원 작업 수는 데스크톱 전원이 켜지는 피크율과 데스크톱이 켜지고, 부팅되고, 연결할 수 있게 될 때까지 소요되는 시간에 따라 결정됩니다. 일반적으로 권장되는 전원 작업 수 제한은 데스크톱이 시작되는 데 소요되는 총 시간에 피크 전원 가동률을 곱한 값입니다.

예를 들어, 데스크톱이 시작되는데 소요되는 평균 시간은 2~3분입니다. 따라서 동시 전원 작업 수 제한은 피크 전원 가동률의 3배가 되어야 합니다. 기본 설정인 50은 분당 16대의 데스크톱 피크 전원 가동률을 지원할 수 있습니다.

시스템에서 데스크톱이 시작될 때까지 최대 5분 동안 기다립니다. 시작 시간이 더 오래 걸릴 경우 다른 오류가 발생할 수 있습니다. 신중을 기하려면 동시 전원 작업 수 제한을 피크 전원 가동률의 5배로 설정하면 됩니다. 신중하게 접근할 경우 기본값인 50으로 설정하여 분당 10대 데스크톱의 피크 전원 가동률을 지원할 수 있습니다.

로그온과 그에 따른 데스크톱 전원 가동 작업은 보통 특정 시간 동안 정규 분포 방식으로 발생합니다. 전원 가동 작업의 약 40%가 해당 시간의 1/6에 발생하므로 피크 전원 가동 작업이 해당 시간의 중간에 발생한다고 추정하여 피크 전원 가동률의 근사치를 계산할 수 있습니다. 예를 들어, 사용자가 오전 8시에서 오전 9시 사이에 로그인할 경우 시간은 1시간이며 로그온의 40%가 오전 8시 25분과 오전 8시 35분 사이의 10분 동안 발생합니다. 사용자가 2,000명이고 20%의 사용자가 데스크톱 전원을 켜려면 400개의 데스크톱 전원 가동 작업의 40%가 이 10분 동안 발생합니다. 따라서 피크 전원 가동률은 분당 16대의 데스크톱입니다.

기본 TLS 인증서의 지문 허용

vCenter Server 및 View Composer 인스턴스를 Horizon 7에 추가할 때 vCenter Server 및 View Composer 인스턴스에 사용되는 TLS 인증서가 유효하고 연결 서버에서 이 인증서를 신뢰하는지 확인해야 합니다. vCenter Server 및 View Composer에 설치된 기본 인증서가 있는 경우 이러한 인증서의 지문을 허용할지 결정해야 합니다.

vCenter Server 또는 View Composer 인스턴스가 CA에서 서명한 인증서로 구성되어 있고 연결 서버가 루트 인증서를 신뢰하는 경우 인증서 지문을 허용하지 않아도 됩니다. 따라서 어떠한 작업도 필요하지 않습니다.

기본 인증서를 CA에서 서명한 인증서로 대체하려 하지만 연결 서버가 루트 인증서를 신뢰하지 않는 경우 인증서 지문을 허용할지 결정해야 합니다. 지문은 인증서의 암호화 해시입니다. 지문은 제시된 인증서가 이전에 허용된 인증서 등의 다른 인증서와 동일한지를 빠르게 결정하는 데 사용됩니다.

참고 동일한 Windows Server 호스트에 vCenter Server 및 View Composer를 설치하는 경우 동일한 TLS 인증서를 사용할 수 있지만 각 구성 요소의 인증서를 별도로 구성해야 합니다.

TLS 인증서 구성에 대한 자세한 내용은 Horizon 7 설치 문서의 “View Server를 위한 TLS 인증서 구성”을 참조하십시오.

먼저 vCenter Server 추가 마법사를 사용해 Horizon Administrator에서 vCenter Server와 View Composer를 추가하십시오. 인증서를 신뢰할 수 없어 지문을 허용하지 않을 경우 vCenter Server와 View Composer를 추가할 수 없습니다.

이러한 서버를 추가한 후에는 vCenter Server 편집 대화상자에서 서버를 재구성할 수 있습니다.

참고 이전 릴리스 및 vCenter Server에서 업그레이드하거나, View Composer 인증서를 신뢰할 수 없거나, 신뢰할 수 있는 인증서를 신뢰할 수 없는 인증서로 바꿀 경우에도 인증서 지문을 허용해야 합니다.

Horizon Administrator 대시보드에서 vCenter Server 또는 View Composer 아이콘이 빨간색으로 바뀌고 [잘못된 인증서가 검색됨] 대화상자가 나타납니다. Horizon Administrator에서 **View 구성 > 서버**를 클릭하고 View Composer 서비스와 연결된 vCenter Server 항목을 편집합니다. 그런 다음 vCenter Server 설정에서 **편집**을 클릭하고 지시에 따라 자체 서명된 인증서를 수락합니다.

마찬가지로 Horizon Administrator에서 연결 서버 인스턴스에 사용할 SAML 인증자를 구성할 수 있습니다. SAML 서버 인증서가 연결 서버에 의해 신뢰되지 않을 경우 인증서 지문을 허용할지 결정해야 합니다. 지문을 허용하지 않으면 Horizon 7에서 SAML 인증자를 구성할 수 없습니다. SAML 인증자가 구성되면 연결 서버 편집 대화 상자에서 인증자를 재구성할 수 있습니다.

절차

- 1 Horizon Administrator에 [잘못된 인증서가 검색됨] 대화상자가 표시되면 **인증서 보기**를 클릭합니다.
- 2 인증서 정보 창에서 인증서 지문을 확인합니다.

- 3 vCenter Server 또는 View Composer 인스턴스에 대해 구성된 인증서 지문을 확인합니다.
 - a vCenter Server 또는 View Composer 호스트에서 MMC 스냅인을 시작하고 Windows 인증서 저장소를 엽니다.
 - b vCenter Server 또는 View Composer 인증서로 이동합니다.
 - c 인증서 세부 정보 탭을 클릭하여 인증서 지문을 표시합니다.

마찬가지로 SAML 인증자의 인증서 지문을 확인합니다. 해당하는 경우 SAML 인증자 호스트에서 앞의 단계를 수행하십시오.
- 4 인증서 정보 창의 지문이 vCenter Server 또는 View Composer 인스턴스의 지문과 일치하는지 확인합니다.

마찬가지로 SAML 인증자의 지문과 일치하는지 확인합니다.
- 5 인증서 지문을 허용할지 결정합니다.

옵션	설명
지문이 일치합니다.	수락을 클릭하여 기본 인증서를 사용합니다.
지문이 일치하지 않습니다.	거부를 클릭합니다. 인증서 불일치 문제를 해결합니다. 예를 들어 vCenter Server 또는 View Composer의 IP 주소를 잘못 입력했을 수 있습니다.

Horizon 7 에서 vCenter Server 인스턴스 제거

Horizon 7와 vCenter Server 인스턴스 사이의 연결을 제거할 수 있습니다. 그럴 경우 Horizon 7는 해당 vCenter Server 인스턴스에 생성된 가상 시스템을 더 이상 관리하지 않습니다.

사전 요구 사항

vCenter Server 인스턴스에 연결된 모든 가상 시스템을 삭제합니다. 가상 시스템 삭제에 대한 자세한 내용은 Horizon 7에서 가상 데스크톱 설정 문서의 “데스크톱 풀 삭제”를 참조하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 클릭합니다.
- 2 **vCenter Server** 탭에서 vCenter Server 인스턴스를 선택합니다.
- 3 **제거**를 클릭합니다.

Horizon 7에는 이제 이 vCenter Server 인스턴스에서 관리하는 가상 시스템에 대한 액세스 권한이 없다는 경고 대화 상자가 나타납니다.

- 4 **확인**을 클릭합니다.

Horizon 7는 vCenter Server 인스턴스에서 생성된 가상 시스템에 더 이상 액세스할 수 없습니다.

Horizon 7 에서 View Composer 제거

Horizon 7와 vCenter Server 인스턴스에 연결된 VMware Horizon View Composer 서비스 간의 연결을 제거할 수 있습니다.

View Composer에 대한 연결을 사용하지 않도록 설정하려면 먼저 View Composer에서 생성된 모든 연결된 클론 가상 시스템을 Horizon 7에서 제거해야 합니다. 연결된 클론이 여전히 연결되어 있는 경우 Horizon 7는 View Composer를 제거하지 못하도록 합니다. View Composer에 대한 연결을 사용하지 않도록 설정한 경우 Horizon 7는 새 연결된 클론을 프로비저닝하거나 관리할 수 없습니다.

절차

- 1 View Composer에서 생성된 연결된 클론 데스크톱 풀을 제거합니다.
 - a Horizon Administrator에서 **카탈로그 > 데스크톱 풀**을 선택합니다.
 - b 연결된 클론 데스크톱 풀을 선택하고 **삭제**를 클릭합니다.
 Horizon 7에서 연결된 클론 데스크톱 풀이 영구적으로 삭제된다는 경고 대화 상자가 나타납니다. 연결된 클론 가상 시스템이 영구 디스크를 사용하여 구성된 경우 영구 디스크를 분리하거나 삭제할 수 있습니다.
 - c **확인**을 클릭합니다.
 가상 시스템이 vCenter Server에서 삭제됩니다. 또한 연결된 View Composer 데이터베이스 항목 및 View Composer에서 생성된 복제본이 삭제됩니다.
 - d View Composer에서 생성된 각 연결된 클론 데스크톱 풀에 대해 이러한 단계를 반복합니다.
- 2 **View 구성 > 서버**를 선택합니다.
- 3 **vCenter Server** 탭에서 View Composer와 연결된 vCenter Server 인스턴스를 선택합니다.
- 4 **편집**을 클릭합니다.
- 5 View Composer Server 설정에서 **편집**을 클릭하고 **View Composer 사용 안 함**을 선택한 다음 **확인**을 클릭합니다.

이 vCenter Server 인스턴스에서 연결된 클론 데스크톱 풀을 더 이상 생성할 수는 없지만 vCenter Server 인스턴스에서 전체 가상 시스템 데스크톱 풀을 계속 생성 및 관리할 수는 있습니다.

다음에 수행할 작업

다른 호스트에 View Composer를 설치하고 새 VMware Horizon View Composer 서비스에 연결하도록 Horizon 7를 재구성하려면 특정 단계를 추가로 수행해야 합니다. [연결된 클론 가상 시스템 없이 View Composer 마이그레이션](#)의 내용을 참조하십시오.

vCenter Server 고유 ID 충돌

환경에 vCenter Server 인스턴스를 여러 개 구성한 경우 고유 ID에서 충돌이 발생해 새 인스턴스를 추가하지 못할 수 있습니다.

문제

Horizon 7에 vCenter Server 인스턴스를 추가할 때 새 vCenter Server 인스턴스의 고유 ID가 기존 인스턴스와 충돌합니다.

원인

두 개의 vCenter Server 인스턴스에서 동일한 고유 ID를 사용할 수 없습니다. 기본적으로 vCenter Server 고유 ID는 임의로 생성되지만 수정할 수 있습니다.

해결책

- 1 vSphere Client에서 **관리 > vCenter Server 설정 > 런타임 설정**을 클릭합니다.
- 2 새 고유 ID를 입력하고 **확인**을 클릭합니다.

vCenter Server 고유 ID 값을 편집하는 자세한 방법은 vSphere 설명서를 참조하십시오.

Horizon 연결 서버 백업

Horizon 연결 서버의 초기 구성을 완료한 후에는 Horizon 7 및 View Composer 구성 데이터의 정기적인 백업을 스케줄링해야 합니다.

Horizon 7 구성 백업 및 복원에 대한 자세한 내용은 [Horizon 7 구성 데이터 백업 및 복원](#)을 참조하십시오.

클라이언트 세션 설정 구성

연결 서버 인스턴스 또는 복제된 그룹에서 관리하는 클라이언트 세션과 연결에 영향을 주는 전역 설정을 구성할 수 있습니다. 세션 시간 초과 길이를 설정하고, 사전 로그인 및 주의 메시지를 표시하고, 보안과 관련된 클라이언트 연결 옵션을 설정할 수 있습니다.

클라이언트 세션 및 연결 옵션 설정

클라이언트 세션 및 연결이 작동하는 방법을 결정하는 전역 설정을 구성합니다.

전역 설정은 단일 연결 서버 인스턴스에 특정하지 않습니다. 독립 실행형 연결 서버 인스턴스 또는 복제된 인스턴스의 그룹에서 관리하는 모든 클라이언트 세션에 영향을 줍니다.

또한 Horizon Client와 원격 데스크톱 사이에 터널링되지 않은 직접 연결을 사용하도록 연결 서버 인스턴스를 구성할 수 있습니다. 직접 연결 구성에 대한 정보는 [보안 터널 및 PCoIP 보안 게이트웨이 구성](#)의 내용을 참조하십시오.

사전 요구 사항

전역 설정을 숙지하십시오. 자세한 내용은 [클라이언트 세션에 대한 전역 설정](#) 및 [클라이언트 세션 및 연결에 대한 전역 보안 설정](#)의 내용을 참조하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 전역 설정**을 선택합니다.
- 2 일반 설정을 구성할지 아니면 보안 설정을 구성할지 선택합니다.

옵션	설명
일반 전역 설정	[일반] 창에서 편집 을 클릭합니다.
전역 보안 설정	보안 창에서 편집 을 클릭합니다.

3 전역 설정을 구성합니다.

4 **확인**을 클릭합니다.

다음에 수행할 작업

설치 중에 제공된 데이터 복구 암호를 변경할 수 있습니다. [데이터 복구 암호 변경](#)의 내용을 참조하십시오.

데이터 복구 암호 변경

데이터 복구 암호는 연결 서버 버전 5.1 이상을 설치할 때 입력해야 합니다. 설치 후에 View Administrator에서 이 암호를 변경할 수 있습니다. 이 암호는 백업에서 View LDAP 구성을 복원할 때 필요합니다.

연결 서버를 백업할 때 View LDAP 구성이 암호화된 LDIF 데이터로 내보내집니다. 암호화된 백업 Horizon 7 구성을 복원하려면 데이터 복구 암호를 입력해야 합니다.

암호는 1 ~ 128자 사이여야 합니다. 조직의 모범 사례에 따라 보안 암호를 생성하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 전역 설정**을 선택합니다.
- 2 보안 창에서 **데이터 복구 암호 변경**을 클릭합니다.
- 3 새 암호를 입력하고 확인합니다.
- 4 (선택 사항) 암호 알림을 입력합니다.

참고 백업할 Horizon 7 구성 데이터를 스케줄링할 때 데이터 복구 암호를 변경할 수도 있습니다. [Horizon 7 구성 백업 예약](#)의 내용을 참조하십시오.

다음에 수행할 작업

vdmimport 유틸리티를 사용하여 백업 Horizon 7 구성을 복원할 때 새 암호를 제공하면 됩니다.

클라이언트 세션에 대한 전역 설정

일반 전역 설정에 따라 세션 시간 초과 길이, SSO 사용 및 시간 초과 제한, Horizon Administrator의 상태 업데이트, 사전 로그인 및 경고 메시지 표시 여부, Horizon Administrator가 Windows Server를 원격 데스크톱에 대해 지원되는 운영 체제로 처리하는지 여부 및 기타 설정 등이 결정됩니다.

아래 표의 설정을 변경하면 해당 변경 내용이 즉시 적용됩니다. Horizon 7 연결 서버 또는 Horizon Client를 다시 시작하지 않아도 됩니다.

표 2-2. 클라이언트 세션에 대한 일반 전역 설정

설정	설명
View Administrator 세션 시간 초과	<p>세션 시간이 초과될 때까지 유효 Horizon Administrator 세션이 지속되는 시간을 결정합니다.</p> <p>중요 Horizon Administrator 세션 시간 초과(단위: 분)를 높게 설정하면 Horizon Administrator를 무단으로 사용할 위험이 높아집니다. 따라서 유효 세션이 오랫동안 지속되도록 허용할 경우 주의해야 합니다.</p> <p>기본적으로 Horizon Administrator 세션 시간 초과는 30분입니다. 세션 시간 초과를 1 ~ 4,320분(72시간)으로 설정할 수 있습니다.</p>
강제로 사용자 연결 끊기	<p>사용자가 Horizon 7에 로그인한 후 지정된 시간(분)이 경과하면 모든 데스크톱 및 애플리케이션의 연결을 끊습니다. 이때 데스크톱과 애플리케이션은 사용자가 언제 열었는지에 관계없이 모두 한꺼번에 연결이 끊어집니다.</p> <p>애플리케이션 원격 작업을 지원하지 않는 클라이언트의 경우 이 설정의 값이 안 함이거나 1,200분보다 크면 최대 시간 초과 값인 1,200분이 적용됩니다.</p> <p>기본값은 600분 후입니다.</p>
SSO(단일 로그인)	<p>SSO를 사용하도록 설정하면 사용자가 원격 Windows 세션에 로그인하기 위한 자격 증명을 제공하지 않고도 원격 데스크톱 또는 애플리케이션을 시작할 수 있도록 Horizon 7에서 사용자의 자격 증명을 캐시에 저장합니다. 기본값은 사용입니다.</p> <p>Horizon 7 이상에 도입된 True SSO 기능을 사용하려는 경우에는 SSO를 사용하도록 설정해야 합니다. True SSO를 사용하면, 사용자가 Active Directory 자격 증명이 아닌 다른 인증 방식을 사용하여 로그인할 경우 사용자가 VMware Identity Manager에 로그인한 후에 True SSO 기능에서 캐시된 자격 증명이 아닌 단기 인증서를 생성합니다.</p> <p>참고 데스크톱이 Horizon Client에서 시작되고 사용자 또는 Windows가 보안 정책을 기반으로 데스크톱을 잠금 경우 그리고 데스크톱에서 Horizon 7 Agent 6.0 이상 또는 Horizon Agent 7.0 이상이 실행되고 있는 경우 Horizon 7 연결 서버는 사용자의 SSO 자격 증명을 삭제합니다. 사용자는 로그인 자격 증명을 제공해야 새 데스크톱 또는 애플리케이션을 시작하거나 연결이 끊어진 데스크톱 또는 애플리케이션에 다시 연결할 수 있습니다. SSO를 다시 사용하도록 설정하려면 사용자가 Horizon 7 연결 서버에서 연결을 끊거나 Horizon Client를 종료했다가 Horizon 7 연결 서버에 다시 연결해야 합니다. 하지만 데스크톱이 Workspace ONE 또는 VMware Identity Manager에서 실행되고 데스크톱이 잠긴 경우에는 SSO 자격 증명이 삭제되지 않습니다.</p>

표 2-2. 클라이언트 세션에 대한 일반 전역 설정 (계속)

설정	설명
<p>애플리케이션을 지원하는 클라이언트의 경우</p> <p>사용자가 키보드와 마우스 사용을 중지하면 해당 애플리케이션의 연결을 끊고 SSO 자격 증명 삭제:</p>	<p>클라이언트 디바이스에서 키보드나 마우스 활동이 없을 때 애플리케이션 세션을 보호합니다. ...분 후로 설정한 경우 Horizon 7에서는 지정된 시간(분) 동안 아무런 사용자 작업이 없으면 모든 애플리케이션의 연결을 끊고 SSO 자격 증명을 삭제합니다. 데스크톱 세션의 연결이 끊어지지 않습니다. 따라서 사용자는 연결이 끊어진 애플리케이션에 로그인하여 다시 연결하거나, 새로운 데스크톱 또는 애플리케이션을 실행해야 합니다.</p> <p>이 설정은 True SSO 기능에도 적용됩니다. SSO 자격 증명이 삭제되고 나면 사용자에게 Active Directory 자격 증명을 요구하는 메시지가 표시됩니다. 사용자가 AD 자격 증명을 사용하지 않고 VMware Identity Manager에 로그인했고 입력할 AD 자격 증명에 무엇인지도 모르는 경우에는 로그아웃했다가 다시 VMware Identity Manager에 로그인하면 원격 데스크톱과 애플리케이션에 액세스할 수 있습니다.</p> <p>중요 사용자는 애플리케이션과 데스크톱이 모두 열려 있는 경우 이 시간 초과로 인해 해당 애플리케이션의 연결은 끊어지더라도 데스크톱은 연결된 상태로 유지된다는 점에 유의해야 합니다. 따라서 이 시간 초과를 사용하여 데스크톱을 보호하면 안 됩니다.</p> <p>안 함으로 설정하면 Horizon 7에서는 사용자 작업이 없어도 애플리케이션 연결을 끊거나 SSO 자격 증명을 삭제하지 않습니다.</p> <p>기본값은 안 함입니다.</p>
<p>기타 클라이언트</p> <p>SSO 자격 증명 삭제:</p>	<p>지정된 시간(분)이 경과한 후 SSO 자격 증명을 삭제합니다. 이 설정은 애플리케이션 원격 작업을 지원하지 않는 클라이언트에 사용됩니다. ...분 후로 설정한 경우 사용자가 클라이언트 디바이스에서 작업 중이더라도 Horizon 7에 로그인한 후 지정된 시간(분)이 경과하면 다시 로그인하여 데스크톱에 연결해야 합니다.</p> <p>안 함으로 설정할 경우 Horizon 7는 사용자가 Horizon Client를 닫거나 강제로 사용자 연결 끊기 시간 초과에 도달할 때까지(둘 중에 빠른 쪽이 적용됨) SSO 자격 증명을 저장합니다.</p> <p>기본값은 15분 후입니다.</p>
자동 상태 업데이트 사용	<p>상태 업데이트가 Horizon Administrator의 왼쪽 위 모서리에 있는 전역 상태 창에 몇 분 단위로 나타나는지 여부를 결정합니다. Horizon Administrator의 대시보드 페이지도 몇 분 단위로 업데이트됩니다.</p> <p>기본적으로 이 설정은 사용하도록 설정되어 있지 않습니다.</p>
사전 로그인 메시지 표시	<p>사용자가 Horizon Client에 로그인할 때 고지 사항 또는 다른 메시지를 표시합니다.</p> <p>전역 설정 대화 상자의 텍스트 상자에 정보 또는 지침을 입력합니다.</p> <p>메시지를 표시하지 않으려면 확인란을 선택 해제하십시오.</p>
강제 로그오프 전에 주의 표시	<p>데스크톱 새로 고침 작업 등과 같은 예약 작업 또는 긴급 업데이트로 인해 사용자가 강제로 로그오프되는 경우 경고 메시지가 표시됩니다. 이 설정은 또한 사용자가 로그오프하기 전에 경고 메시지 표시 시간을 지정합니다.</p> <p>경고 메시지를 표시하려면 확인란을 선택합니다.</p> <p>사용자가 로그오프하기 전에 경고 메시지를 표시할 시간을 분 단위로 입력하십시오.</p> <p>기본값은 5분입니다.</p> <p>경고 메시지를 입력하십시오. 다음과 같은 기본 메시지를 사용할 수 있습니다.</p> <p>중요 업데이트가 예약되어 있기 때문에 데스크톱이 5분 후에 종료됩니다. 저장되지 않은 작업을 지금 저장하십시오.</p>

표 2-2. 클라이언트 세션에 대한 일반 전역 설정 (계속)

설정	설명
Windows Server 데스크톱 사용	<p>사용 가능한 Windows Server 2008 R2 및 Windows Server 2012 R2 시스템을 선택하여 데스크톱으로 사용할 수 있는지 여부를 결정합니다. 이 설정을 사용하도록 설정할 경우 Horizon Administrator는 Horizon 7 서버 구성 요소가 설치된 시스템을 포함하여 사용 가능한 Windows Server 시스템을 모두 표시합니다.</p> <p>참고 Horizon Agent 소프트웨어는 보안 서버, Horizon 7 연결 서버 또는 Horizon 7 Composer를 포함한 다른 Horizon 7 서버 소프트웨어 구성 요소와 동일한 가상 또는 물리적 시스템에 공존할 수 없습니다.</p>
HTML Access에 대한 탭이 닫힐 때 자격 증명 정리	<p>사용자가 원격 데스크톱이나 애플리케이션에 연결하는 탭을 닫거나 HTML Access 클라이언트에서 데스크톱 및 애플리케이션 선택 페이지에 연결하는 탭을 닫을 때 사용자의 자격 증명을 캐시에서 제거합니다.</p> <p>이 설정을 사용하도록 설정하면 Horizon 7에서 다음 HTML Access 클라이언트 시나리오와 같은 경우에도 캐시에 있는 자격 증명을 제거합니다.</p> <ul style="list-style-type: none"> ■ 사용자가 데스크톱 및 애플리케이션 선택 페이지나 원격 세션 페이지를 새로 고칩니다. ■ 서버에서 자체 서명된 인증서를 표시하고, 사용자가 원격 데스크톱 또는 애플리케이션을 실행하고, 보안 경고가 나타났을 때 사용자가 인증서를 승인합니다. ■ 사용자가 원격 세션이 포함된 탭에서 URI 명령을 실행합니다. <p>이 설정을 사용하지 않도록 설정된 경우에는 자격 증명이 캐시에 남아 있습니다. 이 기능은 기본적으로 사용하지 않도록 설정됩니다.</p> <p>참고 이 기능은 Horizon 7 버전 7.0.2 이상에서 사용할 수 있습니다.</p>
Mirage Server 구성	<p>Mirage 서버의 URL을 mirage://서버 이름:포트 또는 mirages://서버 이름:포트 형식으로 지정할 수 있습니다. 여기서 서버 이름은 정규화된 도메인 이름입니다. 포트 번호를 지정하지 않으면 기본 포트 번호인 8000이 사용됩니다.</p> <p>참고 데스크톱 풀 설정에서 Mirage 서버를 지정하여 이 전역 설정을 재정의할 수 있습니다.</p> <p>Mirage 서버를 Horizon Administrator에서 지정하는 것은 Mirage 클라이언트 설치 시 Mirage 서버를 지정하는 것과 동일합니다. Horizon Administrator에서 서버를 지정할 수 있는 Mirage 버전을 확인하려면 https://www.vmware.com/support/pubs/mirage-pubs.html에서 Mirage 설명서를 참조하십시오.</p>
클라이언트 사용자 인터페이스에서 서버 정보 숨기기	<p>Horizon Client 4.4 이상에서 서버 URL 정보를 숨기려면 이 보안 설정을 사용하도록 설정합니다.</p>

표 2-2. 클라이언트 세션에 대한 일반 전역 설정 (계속)

설정	설명
클라이언트 사용자 인터페이스에서 도메인 목록 숨기기	<p>Horizon Client 4.4 이상에서 도메인 드롭다운 메뉴를 숨기려면 이 보안 설정을 사용하도록 설정합니다.</p> <p>클라이언트 사용자 인터페이스에서 도메인 목록 숨기기 전역 설정이 사용되도록 설정된 연결 서버 인스턴스에 사용자가 로그인하는 경우 도메인 드롭다운 메뉴가 Horizon Client에서 숨겨지며 사용자는 Horizon Client 사용자 이름 텍스트 상자에 도메인 정보를 제공합니다. 예를 들어 사용자는 domain\username 또는 username@domain 형식으로 사용자 이름을 입력해야 합니다.</p> <p>중요 클라이언트 사용자 인터페이스에서 도메인 목록 숨기기 설정을 사용하도록 설정하고 연결 서버 인스턴스에 대해 2 요소 인증(RSA SecureID 또는 RADIUS)을 선택하는 경우 Windows 사용자 이름 일치 강제를 적용하지 마십시오. Windows 사용자 이름 일치 적용을 사용하면 사용자가 사용자 이름 텍스트 상자에 도메인 정보를 입력하지 못하므로 로그인이 항상 실패합니다. 단일 사용자 도메인이 있는 경우 Horizon Client 버전 5.0 이상에는 적용되지 않습니다.</p> <p>중요 이 설정의 보안 및 사용성 영향에 대한 자세한 내용은 Horizon 7 보안 문서를 참조하십시오.</p>
도메인 목록 보내기	<p>연결 서버에서 사용자 인증을 위해 클라이언트에 도메인 이름 목록을 보낼 수 있도록 하려면 이 확인란을 선택합니다.</p> <p>중요 이 설정의 보안 및 사용성 영향에 대한 자세한 내용은 Horizon 7 보안 문서를 참조하십시오.</p>

클라이언트 세션 및 연결에 대한 전역 보안 설정

전역 보안 설정에 따라 중단 이후 클라이언트가 재인증되는지 여부, 메시지 보안 모드가 사용되는지 여부 및 IPSec가 보안 서버 연결에 사용되는지 여부가 결정됩니다.

모든 Horizon Client와 Horizon Administrator를 Horizon 7에 연결하려면 TLS가 필요합니다. Horizon 7 배포 시 로드 밸런서나 기타 클라이언트 연결 중간 서버를 사용할 경우 TLS의 부하를 이러한 로드 밸런서나 서버로 분산한 후 개별 연결 서버 인스턴스 및 보안 서버에서 비 TLS 연결을 구성할 수 있습니다. [TLS 연결 부하를 중간 서버로 분산](#)의 내용을 참조하십시오.

표 2-3. 클라이언트 세션 및 연결에 대한 전역 보안 설정

설정	설명
네트워크 중단 후 보안 터널 연결 재인증	<p>Horizon Client에서 보안 터널 연결을 사용해 원격 데스크톱에 연결하는 경우 네트워크 중단 이후 사용자 자격 증명을 재인증해야 할지 여부를 결정합니다.</p> <p>이 설정을 선택할 경우 보안 터널 연결이 중단되면 Horizon Client는 사용자가 다시 연결하기 전에 재인증하도록 요구합니다.</p> <p>이 설정은 보안을 강화합니다. 예를 들어, 도난당한 노트북이 다른 네트워크로 옮겨진 경우 자격 증명을 입력하지 않으면 사용자가 원격 데스크톱에 자동으로 액세스할 수 없습니다.</p> <p>이 설정을 선택하지 않으면 사용자의 재인증 없이 클라이언트가 원격 데스크톱에 다시 연결합니다.</p> <p>보안 터널을 사용하지 않는 경우에는 이 설정이 적용되지 않습니다.</p>
메시지 보안 모드	<p>구성 요소 간에 JMS 메시지를 전송하는 데 사용되는 보안 메커니즘을 결정합니다.</p> <ul style="list-style-type: none"> ■ 모드가 사용으로 설정된 경우 Horizon 7 구성 요소 간에 전송되는 JMS 메시지의 서명 및 확인이 수행됩니다. ■ 모드가 항상으로 설정된 경우 상호 인증된 TLS에서 보안이 제공됩니다. JMS 연결 및 JMS 항목에 대한 액세스 제어. <p>자세한 내용은 Horizon 7 구성 요소의 메시지 보안 모드에 나와 있습니다.</p> <p>신규 설치의 경우 기본적으로 메시지 보안 모드가 항상으로 설정됩니다. 이전 버전에서 업그레이드하는 경우 이전 버전에서 사용된 설정이 유지됩니다.</p>
항상된 보안 상태(읽기 전용)	<p>메시지 보안 모드가 사용에서 항상으로 변경될 때 나타나는 읽기 전용 필드입니다. 단계적으로 변경되기 때문에 이 필드에는 단계에 따른 진행률이 표시됩니다.</p> <ul style="list-style-type: none"> ■ Message Bus 다시 시작을 기다리는 중은 첫 번째 단계입니다. 이 상태는 포드의 모든 연결 서버 호스트에서 VMware Horizon Message Bus 구성 요소 서비스를 수동으로 다시 시작하거나 포드의 모든 연결 서버 인스턴스를 수동으로 다시 시작할 때까지 표시됩니다. ■ 항상 보류 중은 다음 상태입니다. 모든 Horizon Message Bus 구성 요소 서비스가 다시 시작된 후 시스템이 모든 데스크톱 및 보안 서버에 대한 메시지 보안 모드를 항상으로 변경하기 시작합니다. ■ 항상은 최종 상태로, 모든 구성 요소가 이제 항상 메시지 보안 모드를 사용하고 있음을 나타냅니다. <p>vdmutil 명령줄 유틸리티를 사용하여 진행률을 모니터링할 수도 있습니다. vdmutil 유틸리티를 사용하여 JMS 메시지 보안 모드 구성의 내용을 참조하십시오.</p>
보안 서버 연결용 IPsec 사용	<p>IPsec(Internet Protocol Security)를 사용해 보안 서버와 연결 서버 인스턴스를 연결할지 결정합니다.</p> <p>기본적으로 보안 서버 연결용 보안 연결(IPsec 사용)이 사용됩니다.</p>

참고 이전 Horizon 7 릴리스에서 View 5.1 이상으로 업그레이드하는 경우 업그레이드하기 전에 Horizon 7 구성에서 설정을 사용하지 않도록 설정했을 때만 전역 설정 **클라이언트 연결용 SSL 필요**가 Horizon Administrator에 표시됩니다. 모든 Horizon Client와 Horizon Administrator를 Horizon 7에 연결하려면 TLS가 필요하기 때문에 이 설정은 Horizon 7 5.1 이상 버전을 새로 설치하는 경우 표시되지 않으며 이전 Horizon 7 구성에서 설정을 이미 사용하도록 설정한 경우에도 업그레이드 이후 표시되지 않습니다.

업그레이드 이후 **클라이언트 연결용 SSL 필요** 설정을 사용하도록 설정하지 않을 경우 이후 HTTP를 사용하여 연결하도록 구성된 중간 디바이스에 연결하지 않으면 Horizon Client의 HTTPS 연결이 실패합니다. [TLS 연결 부하를 중간 서버로 분산](#)의 내용을 참조하십시오.

Horizon 7 구성 요소의 메시지 보안 모드

메시지 보안 모드를 설정하여 JMS 메시지가 Horizon 7 구성 요소 간에 전송될 때 사용되는 보안 메커니즘을 지정할 수 있습니다.

다음 표에는 메시지 보안 모드 구성 시 선택할 수 있는 옵션이 나와 있습니다. 옵션을 설정하려면 전역 설정 대화 상자 창의 **메시지 보안 모드** 목록에서 선택합니다.

표 2-4. 메시지 보안 모드 옵션

옵션	설명
비활성화됨	메시지 보안 모드를 사용하지 않습니다.
혼합	메시지 보안 모드를 사용하지만 강제로 적용하지 않습니다. 이 모드를 사용하여 Horizon 7 환경에서 Horizon 7 3.0 이전 구성 요소를 검색할 수 있습니다. 연결 서버에서 생성한 로그 파일에 이러한 구성 요소에 대한 참조가 포함되어 있습니다. 이 설정은 권장되지 않습니다. 이 설정은 업그레이드해야 하는 구성 요소를 검색할 때에만 사용합니다.
사용	메시지 보안 모드는 메시지 서명 및 암호화 조합을 사용하여 사용하도록 설정됩니다. 서명이 없거나 잘못된 경우 또는 메시지가 서명 후 수정된 경우 JMS 메시지가 거부됩니다. 일부 JMS 메시지는 사용자 자격 증명과 같은 중요한 정보를 전송하므로 암호화됩니다. 사용 설정을 사용하는 경우 IPsec를 사용하여 연결 서버 인스턴스 간의 그리고 연결 서버 인스턴스와 보안 서버 간의 모든 JMS 메시지를 암호화할 수도 있습니다. 참고 3.0 이전 버전의 Horizon 7 구성 요소는 다른 Horizon 7 구성 요소와 통신할 수 없습니다.
항상	SSL은 모든 JMS 연결에 사용됩니다. 데스크톱, 보안 서버 및 연결 서버 인스턴스가 특정 항목에 대한 JMS 메시지만 전송하고 수신할 수 있도록 JMS 액세스 제어도 사용하도록 설정됩니다. Horizon 6 버전 6.1 이전 Horizon 7 구성 요소는 연결 서버 6.1 인스턴스와 통신할 수 없습니다. 참고 이 모드를 사용하려면 DMZ 기반 보안 서버와 이와 쌍으로 연결된 연결 서버 인스턴스 간에 TCP 포트 4002를 열어야 합니다.

시스템에 Horizon 7을 처음 설치하면 메시지 보안 모드가 **항상**으로 설정됩니다. 이전 릴리스에서 Horizon 7을 업그레이드할 경우 메시지 보안 모드의 기존 설정은 변경되지 않습니다.

중요 업그레이드된 Horizon 7 환경을 **사용**에서 **항상**으로 변경하려는 경우 먼저 모든 연결 서버 인스턴스, 보안 서버 및 Horizon 7 데스크톱을 Horizon 6 버전 6.1 이상 릴리스로 업그레이드해야 합니다. 설정을 **항상**으로 변경한 후 새 설정이 단계적으로 수행됩니다.

- 1 포드의 모든 연결 서버 호스트에서 VMware Horizon View Message Bus 구성 요소 서비스를 수동으로 다시 시작하거나 연결 서버 인스턴스를 다시 시작해야 합니다.
- 2 서비스가 다시 시작된 후 연결 서버 인스턴스는 모드를 **항상**으로 변경하여 모든 데스크톱 및 보안 서버에 대한 메시지 보안 모드를 재구성합니다.
- 3 Horizon Administrator에서 진행률을 모니터링하려면 **View 구성 > 전역 설정**으로 이동합니다.

보안 탭에서 모든 구성 요소가 항상 모드로 전환되면 **항상된 보안 상태** 항목에 **항상**이 표시됩니다.

또는 vdmutil 명령줄 유틸리티를 사용하여 진행률을 모니터링할 수 있습니다. [vdmutil 유틸리티를 사용하여 JMS 메시지 보안 모드 구성](#)의 내용을 참조하십시오.

Horizon 6 버전 6.1 이전 Horizon 7 구성 요소는 항상 모드를 사용하는 연결 서버 6.1 인스턴스와 통신할 수 없습니다.

활성 Horizon 7 환경을 **사용 안 함**에서 **사용**으로 변경하거나 **사용**에서 **사용 안 함**으로 변경할 경우, 마지막으로 변경하기 전에 짧은 시간 동안 **혼합**으로 변경하십시오. 예를 들어, 현재 모드가 **사용 안 함**이면 하루 동안 **혼합** 모드로 변경했다가 **사용**으로 변경하십시오. **혼합** 모드에서는 서명이 메시지에 첨부되지만 확인되지 않으므로 메시지 모드 변경 사항이 환경에 전파됩니다.

vdmutil 유틸리티를 사용하여 JMS 메시지 보안 모드 구성

vdmutil 명령줄 인터페이스를 사용하여 JMS 메시지가 Horizon 7 구성 요소 간에 전송될 때 사용되는 보안 메커니즘을 구성 및 관리할 수 있습니다.

유틸리티의 구문 및 위치

vdmutil 명령은 이전 버전의 Horizon 7에 포함되었던 lmutil 명령과 동일한 작업을 수행할 수 있습니다. 또한 vdmutil 명령에는 사용되고 있는 메시지 보안 모드를 확인하고 모든 Horizon 7 구성 요소를 항상 모드로 변경하는 작업의 진행률을 모니터링하기 위한 옵션이 있습니다. Windows 명령 프롬프트에서 다음 vdmutil 명령 형식을 사용합니다.

```
vdmutil command_option [additional_option argument] ...
```

사용할 수 있는 추가 옵션은 명령 옵션에 따라 다릅니다. 이 항목은 메시지 보안 모드에 대한 옵션을 중점적으로 설명합니다. Cloud Pod 아키텍처와 관련된 기타 옵션은 Horizon 7에서 Cloud Pod 아키텍처 관리 문서를 참조하십시오.

기본적으로 vdmutil 명령 실행 파일의 경로는 C:\Program Files\VMware\VMware View\Server\tools\bin입니다. 명령줄에 경로를 입력하지 않으려면 PATH 환경 변수에 경로를 추가하십시오.

인증

관리자 역할을 가진 사용자로 명령을 실행해야 합니다. Horizon Administrator를 사용하여 사용자에게 관리자 역할을 할당할 수 있습니다. [장6역할 기반 위임된 관리 구성](#)의 내용을 참조하십시오.

vdmutil 명령에는 인증에 사용할 사용자 이름, 도메인 및 암호를 지정하는 옵션이 있습니다.

표 2-5. vdmutil 명령 인증 옵션

옵션	설명
--authAs	Horizon 7 관리자 사용자의 이름입니다. domain\username 또는 UPN(사용자 주체 이름) 형식을 사용하지 마십시오.
--authDomain	--authAs 옵션에 지정된 Horizon 7 관리자 사용자의 정규화된 도메인 이름입니다.
--authPassword	--authAs 옵션에 지정된 Horizon 7 관리자 사용자의 암호입니다. 암호 대신 "*"를 입력하면 vdmutil 명령이 암호를 묻는 메시지를 표시하고 명령줄에서 중요 암호를 명령 기록에 남기지 않습니다.

--help 및 --verbose를 제외한 모든 vdmutil 명령 옵션과 함께 인증 옵션을 사용해야 합니다.

JMS 메시지 보안 모드와 관련된 옵션

다음 표에는 JMS 메시지 보안 모드 보기, 설정 또는 모니터링과 관련된 vdmutil 명령줄 옵션만 나와 있습니다. 특정 옵션과 함께 사용할 수 있는 인수 목록의 경우 --help 명령줄 옵션을 사용합니다.

vdmutil 명령은 작업이 성공하면 0을 반환하고 작업이 실패하면 0이 아닌 장애 관련 코드를 반환합니다. vdmutil 명령은 오류 메시지를 표준 오류로 기록합니다. 작업에서 출력을 생성하거나 자세한 정보 로깅이 --verbose 옵션을 사용하여 사용하도록 설정된 경우 vdmutil 명령은 출력을 표준 출력에 영어로 기록합니다.

표 2-6. vdmutil 명령 옵션

옵션	설명
--activatePendingConnectionServerCertificates	로컬 포드에서 연결 서버 인스턴스에 대해 보류 중인 보안 인증서를 활성화합니다.
--countPendingMsgSecStatus	항상 모드로의 전환 또는 항상 모드에서의 전환을 방지하는 시스템 수를 계산합니다.
--createPendingConnectionServerCertificates	로컬 포드에서 연결 서버 인스턴스에 대해 보류 중인 새 보안 인증서를 생성합니다.
--getMsgSecLevel	로컬 포드에 대한 향상된 메시지 보안 상태를 가져옵니다. 이 상태는 Horizon 7 환경의 모든 구성 요소에 대해 사용 에서 향상 으로 JMS 메시지 보안 모드를 변경하는 프로세스와 관련이 있습니다.
--getMsgSecMode	로컬 포드에 대한 메시지 보안 모드를 가져옵니다.
--help	vdmutil 명령 옵션을 나열합니다. --setMsgSecMode --help와 같은 특정 명령의 --help를 사용할 수도 있습니다.
--listMsgBusSecStatus	로컬 포드에서 모든 연결 서버에 대한 메시지 버스 보안 상태를 나열합니다.
--listPendingMsgSecStatus	항상 모드로의 전환 또는 항상 모드에서의 전환을 방지하는 시스템을 나열합니다. 기본적으로 25개 항목으로 제한됩니다.

표 2-6. vdmutil 명령 옵션 (계속)

옵션	설명
--setMsgSecMode	로컬 포트에 대한 메시지 보안 모드를 설정합니다.
--verbose	자세한 정보 로깅을 사용하도록 설정합니다. 이 옵션을 다른 옵션에 추가하면 자세한 명령 출력을 얻을 수 있습니다. vdmutil 명령은 표준 출력으로 정보를 기록합니다.

보안 터널 및 PCoIP 보안 게이트웨이 구성

보안 터널을 사용하는 경우 사용자가 원격 데스크톱에 연결하면 Horizon Client가 View 연결 서버 또는 보안 서버 호스트에 대한 두 번째 HTTPS 연결을 생성합니다.

PCoIP 보안 게이트웨이를 사용하는 경우 사용자가 PCoIP 디스플레이 프로토콜로 원격 데스크톱에 연결하면 Horizon Client가 연결 서버 또는 보안 서버 호스트에 대한 추가 보안 연결을 생성합니다.

참고 Horizon 6 버전 6.2 이상 릴리스에서는 외부에서 Horizon 6 서버 및 데스크톱에 안전하게 액세스할 수 있도록 보안 서버 대신 Unified Access Gateway 장치를 사용할 수 있습니다. Unified Access Gateway 장치를 사용하는 경우에는 연결 서버 인스턴스에서 보안 게이트웨이를 사용하지 않도록 설정하고 Unified Access Gateway 장치에서 이러한 게이트웨이를 사용하도록 설정할 수 있습니다. 자세한 내용은 Unified Access Gateway 배포 및 구성의 내용을 참조하십시오.

보안 터널 또는 PCoIP 보안 게이트웨이를 사용하도록 설정하지 않은 경우에는 연결 서버 또는 보안 서버 호스트를 건너뛰고 클라이언트 시스템과 원격 데스크톱 가상 시스템 간의 세션이 직접 설정됩니다. 이러한 연결 유형을 직접 연결이라 부릅니다.

중요 외부 클라이언트에 보안 연결을 제공하는 기존 네트워크 구성에는 보안 서버가 포함되어 있습니다. Horizon Administrator를 사용하거나 보안 서버의 보안 터널 및 PCoIP 보안 게이트웨이를 사용하거나 사용하지 않도록 설정하려면 보안 서버에 연결되어 있는 연결 서버 인스턴스를 변경해야 합니다.

외부 클라이언트를 연결 서버 호스트에 직접 연결하는 네트워크 구성에서 Horizon Administrator의 연결 서버 인스턴스를 변경하여 보안 터널과 PCoIP 보안 게이트웨이를 사용하거나 사용하지 않도록 설정할 수 있습니다.

사전 요구 사항

- PCoIP 보안 게이트웨이를 사용하도록 설정할 경우 연결 서버 인스턴스 및 연결된 보안 서버가 Horizon 7 4.6 이상인지 확인하십시오.
- PCoIP 보안 게이트웨이를 이미 사용하도록 설정한 연결 서버 인스턴스와 보안 서버를 연결할 경우 보안 서버가 Horizon 7 4.6 이상인지 확인합니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 **연결 서버** 탭에서 연결 서버 인스턴스를 선택하고 **편집**을 클릭합니다.

3 보안 터널 사용을 구성하십시오.

옵션	설명
보안 터널 사용	보안 터널을 사용하여 시스템에 연결을 선택합니다.
보안 터널 사용 안 함	보안 터널을 사용하여 시스템에 연결을 선택 취소합니다.

기본적으로 보안 터널을 사용하도록 설정되어 있습니다.

4 PCoIP 보안 게이트웨이 사용을 구성하십시오.

옵션	설명
PCoIP 보안 게이트웨이 사용	시스템에 대한 PCoIP 연결에 PCoIP 보안 게이트웨이 사용을 선택합니다.
PCoIP 보안 게이트웨이 사용 안 함	시스템에 대한 PCoIP 연결에 PCoIP 보안 게이트웨이 사용을 선택 취소합니다.

기본적으로 PCoIP 보안 게이트웨이를 사용하지 않도록 설정되어 있습니다.

5 변경 사항을 저장하려면 **확인**을 클릭합니다.

Blast 보안 게이트웨이 구성

Horizon Administrator에서 Blast 보안 게이트웨이의 사용을 구성하면 HTML Access를 통해 또는 VMware Blast 디스플레이 프로토콜을 사용하는 클라이언트 연결을 통해 원격 데스크톱 및 애플리케이션에 대한 보안 액세스를 제공할 수 있습니다.

Blast Secure Gateway에는 속도가 변하고 패킷이 손실되는 등의 네트워크 상태에 맞게 동적으로 조정되는 BEAT(Blast Extreme Adaptive Transport) 네트워킹이 포함됩니다.

- Blast 보안 게이트웨이는 Unified Access Gateway 장치에서 실행될 때만 BEAT 네트워킹을 지원합니다.
- Unified Access Gateway 장치 버전 3.3 이상에 연결할 경우 IPv4를 사용하는 Horizon Client 및 IPv6를 사용하는 Horizon Client는 TCP 포트 8443 및 UDP 포트 8443(BEAT용)에서 동시에 처리될 수 있습니다.
- 일반적인 네트워크 상태를 사용하는 Horizon Client는 연결 서버(BSG 사용 안 함), 보안 서버(BSG 사용 안 함) 또는 2.8 이후 버전의 Unified Access Gateway 장치에 연결해야 합니다. Horizon Client가 일반적인 네트워크 상태를 사용하여 연결 서버(BSG 사용), 보안 서버(BSG 사용) 또는 2.8 이전 버전의 Unified Access Gateway 장치에 연결하는 경우 클라이언트는 네트워크 상태를 자동으로 감지하고 TCP 네트워킹으로 변경합니다.
- 양호하지 않은 네트워크 상태를 사용하는 Horizon Client는 2.9 이상 버전의 Unified Access Gateway 장치(UDP 터널 서버 사용)에 연결해야 합니다. Horizon Client가 양호하지 않은 네트워크 상태를 사용하여 연결 서버(BSG 사용), 보안 서버(BSG 사용) 또는 2.8 이전 버전의 Unified Access Gateway 장치에 연결하는 경우 클라이언트는 네트워크 상태를 자동으로 감지하고 TCP 네트워킹으로 변경합니다.
- Horizon Client가 양호하지 않은 네트워크 상태를 사용하여 연결 서버(BSG 사용 안 함), 보안 서버(BSG 사용 안 함) 또는 버전 2.9 이상의 Unified Access Gateway 장치(UDP 터널 서버 사용 안 함)나 2.8 버전의 Unified Access Gateway 장치에 연결하는 경우 클라이언트는 네트워크 상태를 자동으로 감지하고 일반적인 네트워크 상태로 변경합니다.

자세한 내용은 <https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>에서 Horizon Client 설명서를 참조하십시오.

참고 보안 서버 대신 Unified Access Gateway 장치를 사용하여 Horizon 7 서버 및 데스크톱에 안전하게 외부에서 액세스할 수 있습니다. Unified Access Gateway 장치를 사용하는 경우에는 연결 서버 인스턴스에서 보안 게이트웨이를 사용하지 않도록 설정하고 Unified Access Gateway 장치에서 이러한 게이트웨이를 사용하도록 설정할 수 있습니다. 자세한 내용은 Unified Access Gateway 배포 및 구성의 내용을 참조하십시오.

Blast 보안 게이트웨이가 사용되도록 설정되어 있지 않은 경우에는 클라이언트 디바이스 및 클라이언트 웹 브라우저에서 Blast 보안 게이트웨이를 우회하고 VMware Blast Extreme 프로토콜을 사용하여 원격 데스크톱 가상 시스템 및 애플리케이션에 직접 연결합니다.

중요 외부 사용자에게 보안 연결을 제공하는 일반 네트워크 구성에는 보안 서버가 포함되어 있습니다. 보안 서버의 Blast 보안 게이트웨이를 사용 또는 사용하지 않도록 설정하려면 보안 서버에 연결되어 있는 연결 서버 인스턴스를 편집해야 합니다. 외부 사용자가 연결 서버 호스트에 직접 연결할 경우 연결 서버 인스턴스를 편집하여 Blast 보안 게이트웨이를 사용 또는 사용하지 않도록 설정하십시오.

사전 요구 사항

사용자가 VMware Identity Manager를 통해 원격 데스크톱을 선택할 경우 VMware Identity Manager가 설치되어 있고 연결 서버에서 사용하도록 구성되어 있으며 연결 서버가 SAML 2.0 인증 서버와 연결되어 있는지 확인하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 **연결 서버** 탭에서 연결 서버 인스턴스를 선택하고 **편집**을 클릭합니다.
- 3 Blast 보안 게이트웨이 사용을 구성하십시오.

옵션	설명
Blast 보안 게이트웨이 사용	시스템에 Blast 연결용 Blast 보안 게이트웨이 사용 선택
HTML Access에 대해 Blast 보안 게이트웨이 사용	시스템에 대한 HTML Access Blast 연결에만 Blast 보안 게이트웨이 사용 선택
Blast 보안 게이트웨이 사용 안 함	Blast 보안 게이트웨이 사용 안 함 선택

기본적으로 Blast 보안 게이트웨이를 사용하도록 설정되어 있습니다.

- 4 변경 사항을 저장하려면 **확인**을 클릭합니다.

TLS 연결 부하를 중간 서버로 분산

Horizon Client는 HTTPS를 사용하여 Horizon 7에 연결해야 합니다. Horizon Client가 로드 밸런서나 연결 서버 인스턴스 또는 보안 서버로 연결을 전달하는 다른 중간 서버에 연결할 경우 TLS 부하를 중간 서버로 분산할 수 있습니다.

TLS 부하 분산 서버의 인증서를 Horizon 7 서버로 가져오기

TLS 연결 부하를 중간 서버로 분산하는 경우에는 중간 서버에 연결하는 연결 서버 인스턴스 또는 보안 서버로 중간 서버의 인증서를 가져와야 합니다. 부하 분산 중간 서버와 해당 중간 서버에 연결하는 부하가 분산된 각 Horizon 7 서버에는 동일한 TLS 서버 인증서가 있어야 합니다.

보안 서버를 배포하는 경우에는 중간 서버와 해당 중간 서버에 연결하는 보안 서버에 동일한 TLS 인증서가 있어야 합니다. 보안 서버에 연결되고 중간 서버에 직접 연결하지 않는 연결 서버 인스턴스에는 동일한 TLS 인증서를 설치하지 않아도 됩니다.

보안 서버를 배포하지 않는 경우나 보안 서버와 외부에 연결되는 연결 서버 인스턴스가 혼합되어 있는 네트워크 환경을 사용하는 경우에는 중간 서버와 해당 중간 서버에 연결하는 모든 연결 서버 인스턴스에 동일한 TLS 인증서가 있어야 합니다.

중간 서버의 인증서가 연결 서버 인스턴스나 보안 서버에 설치되어 있지 않으면 클라이언트가 Horizon 7에 대한 연결의 유효성을 검사할 수 없습니다. 이 경우에는 Horizon 7 서버에서 전송한 인증서 지문이 Horizon Client가 연결하는 중간 서버의 인증서와 일치하지 않습니다.

로드 밸런싱과 TLS 부하 분산을 혼동하지 마십시오. 위의 요건은 몇몇 유형의 로드 밸런서를 포함해 TLS 부하 분산을 제공하도록 구성된 디바이스에 적용됩니다. 그러나 순수 로드 밸런싱에는 디바이스 간 인증서 복사가 필요하지 않습니다.

Horizon 7 서버로 인증서를 가져오는 방법에 대한 자세한 내용은 Horizon 7 설치 문서에서 "Windows 인증서 저장소에 서명된 서버 인증서 가져오기"를 참조하십시오.

클라이언트가 TLS 부하 분산 서버를 가리키도록 Horizon 7 Server 외부 URL 설정

TLS의 부하가 중간 서버로 분산되고 Horizon Client 디바이스가 보안 터널을 사용하여 Horizon 7에 연결하는 경우, 보안 터널 외부 URL을 클라이언트가 중간 서버에 액세스하는 데 사용할 수 있는 주소로 설정해야 합니다.

중간 서버에 연결하는 연결 서버 인스턴스 또는 보안 서버의 외부 URL 설정을 구성합니다.

보안 서버를 배포하는 경우, 외부 URL은 보안 서버에만 필요하고 보안 서버와 연결되는 연결 서버 인스턴스에는 필요하지 않습니다.

보안 서버를 배포하지 않는 경우나 보안 서버와 외부에 연결되는 연결 서버 인스턴스가 혼합되어 있는 네트워크 환경을 사용하는 경우에는 중간 서버에 연결하는 모든 연결 서버 인스턴스에 외부 URL이 필요합니다.

참고 PCoIP 보안 게이트웨이(PSG) 또는 Blast 보안 게이트웨이를 사용하는 TLS 연결의 부하를 분산할 수 없습니다. PCoIP 외부 URL과 Blast 보안 게이트웨이 외부 URL은 클라이언트가 PSG 및 Blast 보안 게이트웨이를 호스트하는 컴퓨터에 연결할 수 있도록 허용해야 합니다. 중간 서버와 Horizon 7 Server 사이에 TLS 연결을 요구할 계획이 아니라면 PCoIP 외부 URL과 Blast 외부 URL이 중간 서버를 가리키도록 재설정하지 마십시오.

외부 URL 구성에 대한 자세한 내용은 Horizon 7 설치 문서에서 "PCoIP 보안 게이트웨이 및 터널 연결용 외부 URL 구성"을 참조하십시오.

중간 서버의 HTTP 연결 허용

TLS의 부하가 중간 서버로 분산되는 경우 클라이언트 쪽 중간 디바이스의 HTTP 연결을 허용하도록 연결 서버 인스턴스나 보안 서버를 구성할 수 있습니다. 중간 디바이스는 Horizon Client 연결에 대해 HTTPS를 허용해야 합니다.

Horizon 7 서버와 중간 디바이스 사이에 HTTP 연결을 허용하려면 HTTP 연결이 허용되는 각 연결 서버와 보안 서버에서 `locked.properties` 파일을 구성해야 합니다.

Horizon 7 서버와 중간 디바이스 사이에 HTTP 연결을 허용하더라도 Horizon 7에서 TLS를 사용하지 않도록 설정할 수는 없습니다. Horizon 7 서버에서는 HTTP 연결뿐 아니라 HTTPS 연결도 계속해서 수락합니다.

참고 Horizon 클라이언트에서 스마트 카드 인증을 사용하는 경우, 연결 서버나 보안 서버에 대해 직접 HTTPS 연결을 설정해야 합니다. 스마트 카드 인증을 사용하면 TLS 부하 분산 기능이 지원되지 않습니다.

절차

- 1 연결 서버 또는 보안 서버 호스트의 TLS/SSL 게이트웨이 구성 폴더에 `locked.properties` 파일을 생성 또는 편집합니다.
예: `install_directory\VMware\VMware View\Server\SSLgateway\conf\locked.properties`
- 2 Horizon 7 서버의 프로토콜을 구성하려면 `serverProtocol` 속성을 추가하고 `http`로 설정합니다.
`http` 값은 소문자로 입력해야 합니다.
- 3 (선택 사항) Horizon 7 서버에 기본값이 아닌 HTTP 수신 포트와 네트워크 인터페이스를 구성하는 속성을 추가합니다.
 - HTTP 수신 포트 80에서 변경하려면 `serverPortNonTLS`를 중간 디바이스가 연결할 수 있도록 구성한 다른 포트 번호로 설정합니다.
 - Horizon 7 서버에 네트워크 인터페이스가 2개 이상 있는 경우에 서버가 하나의 인터페이스에서만 HTTP 연결을 수신하도록 하려면 해당 네트워크 인터페이스의 IP 주소를 `serverHostNonTLS`에 설정합니다.
- 4 `locked.properties` 파일을 저장합니다.
- 5 변경 내용을 적용하려면 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작합니다.

예제: `locked.properties` 파일

이 파일을 사용하면 Horizon 7 서버에 TLS가 아닌 HTTP 연결을 사용할 수 있습니다. Horizon 7 서버의 클라이언트 쪽 네트워크 인터페이스의 IP 주소는 10.20.30.40입니다. 서버는 기본 포트 80을 사용하여 HTTP 연결을 수신합니다. `http` 값은 소문자로 입력해야 합니다.

```
serverProtocol=http
serverHostNonTLS=10.20.30.40
```


Horizon 연결 서버나 보안 서버 호스트의 게이트웨이 위치 구성

기본적으로 Horizon 연결 서버 인스턴스는 게이트웨이 위치를 내부로 설정하고 보안 서버는 게이트웨이 위치를 외부로 설정합니다. `locked.properties` 파일에 `gatewayLocation` 속성을 설정해서 기본 게이트웨이 위치를 변경했습니다.

게이트웨이 위치는 원격 데스크톱에서 `ViewClient_Broker_GatewayLocation` 레지스트리 키 값을 결정합니다. 이 값을 스마트 정책에 사용하면 사용자가 회사 네트워크의 내부/외부에서 원격 데스크톱에 연결한 경우에만 정책을 적용하도록 구성할 수 있습니다. 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성 문서의 “스마트 정책 사용”을 참조하십시오.

절차

- 1 Horizon 연결 서버 또는 보안 서버 호스트의 TLS/SSL 게이트웨이 구성 폴더에 `locked.properties` 파일을 생성 또는 편집합니다.

예: `install_directory\VMware\VMware View\Server\ssl\gateway\conf\locked.properties`

`locked.properties` 파일의 속성은 대/소문자를 구분합니다.

- 2 다음 행을 `locked.properties` 파일에 추가하십시오.

`gatewayLocation=value`

`value`는 `External`(외부) 또는 `Internal`(내부)일 수 있습니다. `External`(외부)는 회사 네트워크 외부의 사용자가 사용할 수 있는 게이트웨이입니다. `Internal`(내부)는 회사 네트워크 내부의 사용자가 사용할 수 있는 게이트웨이입니다.

예: `gatewayLocation=External`

- 3 `locked.properties` 파일을 저장합니다.
- 4 변경 사항을 적용하려면 VMware Horizon 연결 서버 서비스 또는 VMware Horizon 보안 서버 서비스를 다시 시작합니다.

Horizon 연결 서버를 사용 또는 사용하지 않도록 설정

연결 서버 인스턴스를 사용하지 않도록 설정하면 사용자가 가상 또는 게시된 데스크톱 및 애플리케이션에 로그인할 수 없습니다. 인스턴스를 사용하지 않도록 설정한 후에 다시 사용하도록 설정할 수 있습니다.

연결 서버 인스턴스를 사용하지 않도록 설정해도 데스크톱 및 애플리케이션에 현재 로그인된 사용자에게는 영향이 미치지 않습니다.

Horizon 7 배포에 따라 인스턴스를 사용하지 않도록 설정했을 때 사용자에게 미치는 영향이 결정됩니다.

- 단일, 독립 실행형 연결 서버 인스턴스의 경우 사용자는 데스크톱 또는 애플리케이션에 로그인할 수 없습니다. 연결 서버에 연결할 수 없습니다.

- 복제된 연결 서버 인스턴스의 경우 네트워크 토폴로지에 따라 사용자가 다른 복제된 인스턴스로 라우팅할 수 있을지 여부가 결정됩니다. 사용자가 다른 인스턴스에 액세스할 수 있으면 데스크톱 및 애플리케이션에 로그인할 수 있습니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 **연결 서버** 탭에서 연결 서버 인스턴스를 선택합니다.
- 3 **사용 안 함**을 클릭합니다.

사용을 클릭해 인스턴스를 사용하도록 설정할 수 있습니다.

외부 URL 편집

Horizon Administrator를 사용해 연결 서버 인스턴스 및 보안 서버에 대한 외부 URL을 편집할 수 있습니다.

기본적으로 연결 서버 또는 보안 서버 호스트는 동일한 네트워크에 있는 터널 클라이언트로만 연결할 수 있습니다. 네트워크 밖에서 실행하는 터널 클라이언트는 클라이언트가 확인할 수 있는 URL을 사용해 연결 서버 또는 보안 서버 호스트에 연결해야 합니다.

사용자가 PCoIP 디스플레이 프로토콜을 사용하여 원격 데스크톱에 연결한 경우 Horizon Client는 연결 서버나 보안 서버 호스트에서 PCoIP 보안 게이트웨이에 대한 추가 연결을 생성할 수 있습니다. PCoIP 보안 게이트웨이를 사용하려면 클라이언트 시스템에서 클라이언트가 연결 서버 또는 보안 서버 호스트에 연결하는데 사용하는 IP 주소에 액세스할 수 있어야 합니다. PCoIP 외부 URL에서 이 IP 주소를 지정합니다.

세 번째는 사용자가 Blast 보안 게이트웨이를 통해 보안 연결할 수 있는 URL입니다.

보안 터널 외부 URL, PCoIP 외부 URL 및 Blast 외부 URL은 클라이언트 시스템이 이 호스트에 도달하기 위해 사용하는 주소여야 합니다.

참고 연결 서버 4.5 이상으로 업그레이드하지 않은 보안 서버에 대해서는 외부 URL을 편집할 수 없습니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.

옵션	조치
View 연결 서버 인스턴스	연결 서버 탭에서 연결 서버 인스턴스를 선택하고 편집 을 클릭합니다.
보안 서버	보안 서버 탭에서 보안 서버를 선택하고 편집 을 클릭합니다.

2 외부 URL 텍스트 상자에 보안 터널 외부 URL을 입력합니다.

URL에는 프로토콜, 클라이언트가 확인 가능한 호스트 이름 및 포트 번호가 포함되어야 합니다.

예: `https://view.example.com:443`

참고 호스트 이름을 확인할 수 없는 경우, 연결 서버 인스턴스나 보안 서버에 액세스할 수 있으면 IP 주소를 사용할 수 있습니다. 그러나 연결하는 호스트가 연결 서버 인스턴스나 보안 서버에 구성되어 있는 SSL 인증서와 일치하지 않게 되어 액세스가 차단되거나 낮은 수준의 보안을 사용하여 액세스하게 됩니다.

3 PCoIP 외부 URL 텍스트 상자에 PCoIP 보안 게이트웨이 외부 URL을 입력합니다.

포트 번호 4172를 가진 IP 주소로 PCoIP 외부 URL을 지정합니다. 프로토콜 이름은 포함시키지 마십시오.

예: `10.20.30.40:4172`

URL에는 클라이언트 시스템에서 보안 서버 또는 연결 서버 인스턴스에 연결할 때 사용하는 IP 주소와 포트 번호가 포함되어 있어야 합니다.

4 Blast 외부 URL 텍스트 상자에 Blast 보안 게이트웨이 외부 URL을 입력하십시오.

URL에는 HTTPS 프로토콜, 클라이언트가 확인 가능한 호스트 이름 및 포트 번호가 포함되어야 합니다.

예: `https://myserver.example.com:8443`

기본적으로 URL에는 보안 터널 외부 URL의 FQDN과 기본 포트 번호 8443이 포함됩니다.

URL에는 클라이언트 시스템이 이 호스트에 도달하기 위해 사용할 수 있는 FQDN과 포트 번호가 포함되어야 합니다.

5 이 대화 상자의 모든 주소가 클라이언트 시스템이 이 호스트에 도달하도록 허용하는지 확인합니다.

6 변경 사항을 저장하려면 **확인**을 클릭합니다.

외부 URL이 즉시 업데이트됩니다. 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작하지 않아도 변경 내용이 적용됩니다.

고객 환경 개선 프로그램 참여 또는 철회

새 구성을 사용하여 연결 서버를 설치할 경우 고객 환경 향상 프로그램에 참여하도록 선택할 수 있습니다. 설치 후 참여 의사가 바뀔 경우 Horizon Administrator를 사용하여 프로그램에 대한 참여 여부를 지정할 수 있습니다.

프로그램에 참여할 경우 VMware는 사용자 요구 사항에 대한 VMware의 응답을 개선하기 위해 배포 환경에 관한 데이터를 익명으로 수집합니다. 조직을 식별할 수 있는 데이터는 수집하지 않습니다.

익명 필드 등 데이터가 수집되는 필드 목록을 검토하려면 [GUID-4FDD21B3-5F28-419F-AA16-4C7578996A54#GUID-4FDD21B3-5F28-419F-AA16-4C7578996A54](#)를 참조하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 제품 라이선싱 및 사용량**을 선택합니다.
- 2 고객 환경 개선 프로그램 창에서 **설정 편집**을 클릭합니다.
- 3 **VMware에 익명 데이터 보내기** 확인란을 선택하거나 선택 취소하여 프로그램에 대한 참여 여부를 결정합니다.
- 4 (선택 사항) 참여할 경우 조직의 지리적 위치, 비즈니스 유형 및 직원 수를 선택할 수 있습니다.
- 5 **확인**을 클릭합니다.

View LDAP 디렉토리

View LDAP는 모든 Horizon 7 구성 정보의 데이터 저장소입니다. View LDAP는 연결 서버 설치와 함께 제공되는 내장된 LDAP(Lightweight Directory Access Protocol) 디렉토리입니다.

View LDAP에는 Horizon 7에서 사용되는 표준 LDAP 디렉토리 구성 요소가 포함되어 있습니다.

- Horizon 7 스키마 정의
- DIT(Directory Information Tree) 정의
- 액세스 제어 목록(ACL)

View LDAP에는 Horizon 7 개체를 나타내는 디렉토리 항목이 포함됩니다.

- 액세스 가능한 각 데스크톱을 나타내는 원격 데스크톱 항목. 각 항목은 데스크톱을 사용하도록 인증 받은 Active Directory의 Windows 사용자 및 그룹의 외부 보안 주체(FSP)에 대한 참조를 포함합니다.
- 함께 관리되는 다수의 데스크톱을 나타내는 원격 데스크톱 풀 항목.
- 각 원격 데스크톱의 vCenter Server 가상 시스템을 나타내는 가상 시스템 항목
- 구성 설정을 저장하는 Horizon 7 구성 요소 항목

View LDAP에는 다른 Horizon 7 구성 요소의 자동화 및 알림 서비스를 제공하는 Horizon 7 플러그인 DLL 집합도 포함되어 있습니다.

참고 보안 서버 인스턴스는 View LDAP 디렉토리를 포함하지 않습니다.

LDAP 복제

연결 서버의 복제된 인스턴스를 설치할 때 Horizon 7은 기존 연결 서버 인스턴스에서 View LDAP 구성 데이터를 복제합니다. 동일한 View LDAP 구성 데이터가 복제된 그룹의 모든 연결 서버 인스턴스에서 유지됩니다. 인스턴스 1개에서 내용을 변경하면 다른 인스턴스에 업데이트 정보가 복사됩니다.

복제된 인스턴스가 잘못된 경우 그룹의 다른 인스턴스에서 작업을 계속합니다. 잘못된 인스턴스가 다시 작업을 시작하면 운영을 중단했던 동안 변경된 구성이 업데이트됩니다. Horizon 7 이상 릴리스에서는 15분 간격으로 복제 상태 확인을 수행하여 각 인스턴스가 복제된 그룹의 다른 서버와 통신할 수 있는지, 그리고 각 인스턴스가 그룹에 있는 다른 서버에서 LDAP 업데이트를 가져올 수 있는지 확인합니다.

Horizon Administrator에서 대시보드를 사용하여 복제 상태를 확인할 수 있습니다. 연결 서버 인스턴스 중에 대시보드에서 빨간색 아이콘이 표시된 것이 있으면 아이콘을 클릭하여 복제 상태를 확인합니다. 복제는 다음과 같은 이유로 손상될 수 있습니다.

- 방화벽으로 인한 통신 차단
- VMware VDMDS 서비스가 연결 서버 인스턴스에서 중단되었을 수 있습니다.
- VMware VDMDS DS 옵션이 복제를 차단할 수 있음
- 네트워크 문제 발생

기본적으로 복제 확인은 15분마다 이루어집니다. 연결 서버 인스턴스에서 ADSI 편집을 사용하면 간격을 변경할 수 있습니다. 시간을 분 단위로 설정하려면 **DC=vdi,DC=vmware,DC=int**에 연결하고 **CN=Common,OU=Global,OU=Properties** 개체에서 **pae-ReplicationStatusDataExpiryInMins** 특성을 편집합니다.

pae-ReplicationStatusDataExpiryInMins 특성 값은 10분에서 1440분(하루) 사이에 있어야 합니다. 특성 값이 10분 미만이면 Horizon 7에서 10분으로 처리합니다. 특성 값이 1440분을 넘는 경우는 Horizon 7에서 1440분으로 처리합니다.

스마트 카드 인증 설정

보안 강화를 위해, 사용자와 관리자가 스마트 카드를 사용하여 인증할 수 있도록 연결 서버 인스턴스 또는 보안 서버를 구성할 수 있습니다.

스마트 카드는 컴퓨터 칩이 포함된 소형 플라스틱 카드입니다. 소형 컴퓨터와 같은 칩에는 개인 키 및 공용 키 인증서를 포함한 데이터의 보안 스토리지가 포함됩니다. 미국 국방부에서 사용하는 한 가지 유형의 스마트 카드를 CAC(Common Access Card)라고 합니다.

스마트 카드 인증을 사용할 경우, 사용어나 관리자는 클라이언트 컴퓨터에 연결된 스마트 카드 판독기에 스마트 카드를 삽입하고 PIN을 입력해야 합니다. 스마트 카드 인증은 사용자가 가진 정보(스마트 카드)와 사용자가 아는 정보(PIN)를 모두 확인하여 2 요소 인증을 제공합니다.

스마트 카드 인증을 구현하기 위한 하드웨어 및 소프트웨어 요구 사항에 대한 정보는 Horizon 7 설치 문서를 참조하십시오. Microsoft TechNet 웹 사이트에는 Windows 시스템의 스마트 카드 인증 계획 및 구현에 대한 자세한 정보가 포함되어 있습니다.

스마트 카드를 사용하려면 클라이언트 시스템에 스마트 카드 미들웨어 및 스마트 카드 판독기가 있어야 합니다. 스마트 카드에 인증서를 설치하려면 등록 스테이션 역할을 하도록 컴퓨터를 설정해야 합니다.

특정 유형의 Horizon Client가 스마트 카드를 지원하는지 여부에 대한 자세한 내용은 <https://docs.vmware.com/kr/VMware-Horizon-Client/index.html>에 있는

Horizon Client 설명서를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [스마트 카드를 사용하여 로그인](#)
- [Horizon 연결 서버에서 스마트 카드 인증 구성](#)
- [타사 솔루션에서 스마트 카드 인증 구성](#)
- [스마트 카드 인증을 위한 Active Directory 준비](#)
- [스마트 카드 인증 구성 확인](#)
- [스마트 카드 인증서 해지 검사 사용](#)

스마트 카드를 사용하여 로그인

사용자나 관리자가 스마트 카드 판독기에 스마트 카드를 삽입하면 클라이언트 운영 체제가 Windows 인 경우 스마트 카드의 사용자 인증서가 클라이언트 시스템의 로컬 인증서 저장소로 복사됩니다.

Horizon Client를 포함해 클라이언트 컴퓨터에서 실행 중인 모든 애플리케이션에서 로컬 인증서 저장소의 인증서를 사용할 수 있습니다.

사용자나 관리자가 스마트 카드 인증용으로 구성된 보안 서버 또는 연결 서버 인스턴스에 대한 연결을 시작하면 보안 서버 또는 연결 서버 인스턴스에서 클라이언트 시스템으로 신뢰할 수 있는 CA(인증 기관) 목록이 전송됩니다. 클라이언트 시스템은 신뢰할 수 있는 CA 목록에서 사용 가능한 사용자 인증서를 확인하고 적당한 인증서를 선택한 다음 사용자나 관리자에게 스마트 카드 PIN을 입력하라는 메시지를 표시합니다. 유효한 사용자 인증서가 여러 개인 경우에는 사용자나 관리자에게 인증서를 선택하라는 메시지가 표시됩니다.

클라이언트 시스템이 사용자 인증서를 전송하면 보안 서버 또는 연결 서버 인스턴스가 인증서 신뢰성 및 유효 기간을 확인해 인증서를 검증합니다. 일반적으로 서명되어 있고 유효한 사용자 인증서를 사용하면 사용자와 관리자가 성공적으로 인증받을 수 있습니다. 인증서 해지 확인을 구성하면 사용자 인증서를 해지한 사용자나 관리자가 인증을 받을 수 없습니다.

일부 환경에서는 사용자의 스마트 카드 인증서가 여러 Active Directory 도메인 사용자 계정으로 매핑될 수도 있습니다. 사용자에게 관리자 권한을 가진 계정 여러 개가 있어서 스마트 카드 로그인 시 [사용자 이름 힌트] 필드에 사용할 계정을 지정해야 할 수도 있습니다. Horizon Client 로그인 대화 상자에 [사용자 이름 힌트] 필드가 나타나게 하려면 관리자가 Horizon Administrator의 연결 서버 인스턴스에서 스마트 카드 사용자 이름 힌트 기능을 사용하도록 설정해야 합니다. 그러면 스마트 카드 사용자는 스마트 카드 로그인 시 [사용자 이름 힌트] 필드에 사용자 이름이나 UPN을 입력할 수 있습니다.

작업 환경에서 보안 외부 액세스를 위해 Unified Access Gateway 장치를 사용하는 경우 스마트 카드 사용자 이름 힌트 기능을 지원하도록 Unified Access Gateway 장치를 구성해야 합니다. 스마트 카드 사용자 이름 힌트 기능은 Unified Access Gateway 버전 2.7.2 이상에서만 지원됩니다.

Unified Access Gateway 장치의 스마트 카드 사용자 이름 힌트 기능을 사용하도록 설정하는 방법에 대한 자세한 내용은 Unified Access Gateway 배포 및 구성 문서를 참조하십시오.

Horizon Client에서 스마트 카드로 인증하면 디스플레이 프로토콜을 전환할 수 없습니다.

Horizon Client에서 스마트 카드로 인증한 후 디스플레이 프로토콜을 변경하려면 사용자가 로그오프했다가 다시 로그인해야 합니다.

Horizon 연결 서버에서 스마트 카드 인증 구성

스마트 카드 인증을 구성하려면 루트 인증서를 가져와 서버 truststore 파일에 추가한 다음, 연결 서버 구성 속성을 수정하고 스마트 카드 인증 설정을 구성해야 합니다. 사용자 환경에 따라 추가 작업을 수행해야 하는 경우도 있습니다.

절차

1 인증 기관 인증서 가져오기

사용자와 관리자가 제공한 스마트 카드의 신뢰할 수 있는 모든 사용자 인증서에 대해 적용 가능한 모든 CA(인증 기관) 인증서를 가져와야 합니다. 이러한 인증서에는 루트 인증서가 포함되며, 사용자의 스마트 카드 인증서가 중간 인증 기관에서 발급된 경우에는 중간 인증서도 포함될 수 있습니다.

2 Windows에서 CA 인증서 가져오기

CA 서명이 있는 사용자 인증서 또는 이 인증서가 포함된 스마트 카드가 있으면 Windows가 루트 인증서를 신뢰하기 때문에 Windows에서 루트 인증서를 내보낼 수 있습니다. 사용자 인증서의 발급자가 중간 인증 기관인 경우에는 해당 인증서를 내보낼 수 있습니다.

3 서버 Truststore 파일에 CA 인증서 추가

신뢰하는 사용자와 관리자 모두의 루트 인증서, 중간 인증서 또는 둘 모두를 서버 truststore 파일에 추가해야 합니다. 연결 서버 인스턴스와 보안 서버는 이 정보를 사용하여 스마트 카드 사용자와 관리자를 인증합니다.

4 Horizon 연결 서버 구성 속성 수정

스마트 카드 인증을 사용하도록 설정하려면 연결 서버 또는 보안 서버 호스트에서 연결 서버 구성 속성을 수정해야 합니다.

5 Horizon Administrator에서 스마트 카드 설정 구성

Horizon Administrator를 사용해 다른 스마트 카드 인증 시나리오를 수용하도록 설정할 수 있습니다.

인증 기관 인증서 가져오기

사용자와 관리자가 제공한 스마트 카드의 신뢰할 수 있는 모든 사용자 인증서에 대해 적용 가능한 모든 CA(인증 기관) 인증서를 가져와야 합니다. 이러한 인증서에는 루트 인증서가 포함되며, 사용자의 스마트 카드 인증서가 중간 인증 기관에서 발급된 경우에는 중간 인증서도 포함될 수 있습니다.

사용자와 관리자가 제공한 스마트 카드에 있는 인증서를 서명한 CA의 루트 또는 중간 인증서가 없는 경우 인증서가 들어 있는 스마트 카드 또는 CA 서명 사용자 인증서에서 해당 인증서를 내보낼 수 있습니다. [Windows에서 CA 인증서 가져오기](#)의 내용을 참조하십시오.

절차

- ◆ 다음 소스 중 하나에서 CA 인증서를 가져오십시오.
 - Microsoft Certificate Services를 실행 중인 Microsoft IIS 서버. Microsoft IIS 설치, 인증서 발행 및 조직의 인증서 배포에 대한 정보는 Microsoft TechNet 웹사이트를 참조하십시오.
 - 신뢰된 CA의 공용 루트 인증서. 이는 이미 스마트 카드 인프라가 있는 환경에서 루트 인증서의 가장 일반적인 소스이며 스마트 카드 분산 및 인증에 대한 표준화된 접근법입니다.

다음에 수행할 작업

서버 Truststore 파일에 루트 인증서, 중간 인증서 또는 둘 모두를 추가하십시오.

Windows에서 CA 인증서 가져오기

CA 서명이 있는 사용자 인증서 또는 이 인증서가 포함된 스마트 카드가 있으면 Windows가 루트 인증서를 신뢰하기 때문에 Windows에서 루트 인증서를 내보낼 수 있습니다. 사용자 인증서의 발급자가 중간 인증 기관인 경우에는 해당 인증서를 내보낼 수 있습니다.

절차

- 1 스마트 카드에 사용자 인증서가 있는 경우 개인 저장소에 사용자 인증서를 추가하려면 판독기에 스마트 카드를 삽입하십시오.

개인 저장소에 사용자 인증서가 표시되지 않는 경우에는 판독기 소프트웨어를 사용해 사용자 인증서로 파일로 내보내십시오. 이 파일은 이 절차의 4단계에서 사용됩니다.

2 Internet Explorer에서 **도구 > 인터넷 옵션**을 선택합니다.

3 **내용** 탭에서 **인증서**를 클릭합니다.

4 **개인** 탭에서 사용할 인증서를 선택하고 **보기**를 클릭합니다.

목록에 사용자 인증서가 표시되지 않으면 **가져오기**를 클릭해 파일에서 수동으로 인증서를 가져오십시오. 인증서를 가져온 후에 목록에서 인증서를 선택할 수 있습니다.

5 **인증 경로** 탭에서 트리 맨 위에 있는 인증서를 선택하고 **인증서 보기**를 클릭합니다.

사용자 인증서가 트러스트 계층 구조의 일부로 서명된 경우에는 다른 고수준 인증서에서 서명 인증서에 서명했을 수 있습니다. 상위 인증서(실제로 사용자 인증서에 서명한 인증서)를 루트 인증서로 선택합니다. 경우에 따라 발급자가 중간 CA일 수도 있습니다.

6 **세부 정보** 탭에서 **파일에 복사**를 클릭합니다.

인증서 내보내기 마법사가 나타납니다.

7 **다음 > 다음**을 클릭하고 내보낼 파일의 이름과 위치를 입력합니다.

8 파일을 지정한 위치로 루트 인증서로 저장하려면 **다음**을 클릭합니다.

다음에 수행할 작업

서버 Truststore 파일에 CA 인증서를 추가합니다.

서버 Truststore 파일에 CA 인증서 추가

신뢰하는 사용자와 관리자 모두의 루트 인증서, 중간 인증서 또는 둘 모두를 서버 truststore 파일에 추가해야 합니다. 연결 서버 인스턴스와 보안 서버는 이 정보를 사용하여 스마트 카드 사용자와 관리자를 인증합니다.

사전 요구 사항

- 사용자 또는 관리자가 제공한 스마트 카드의 인증서에 서명하는 데 사용된 루트 또는 중간 인증서를 가져옵니다. 자세한 내용은 [인증 기관 인증서 가져오기](#) 및 [Windows에서 CA 인증서 가져오기](#)의 내용을 참조하십시오.

중요 이러한 인증서에는 사용자의 스마트 카드 인증서가 중간 인증 기관에서 발급된 경우, 중간 인증서도 포함될 수 있습니다.

- 연결 서버 또는 보안 서버 호스트의 시스템 경로에 keytool 유틸리티가 추가되었는지 확인하십시오. 자세한 내용은 Horizon 7 설치 문서를 참조하십시오.

절차

- 1 연결 서버 또는 보안 서버 호스트에서 keytool 유틸리티를 사용해 루트 인증서, 중간 인증서 또는 둘 모두를 서버 truststore 파일로 가져오십시오.

예: `keytool -import -alias alias -file root_certificate -keystore truststorefile.key`

이 명령에서 alias는 truststore 파일의 새 항목에 대한 고유한 이름으로, 대소문자가 구분되며 root_certificate는 가져오거나 내보낸 루트 또는 중간 인증서이고 truststorefile.key는 루트 인증서를 추가할 truststore 파일 이름입니다. 파일이 없으면 현재 디렉토리에 생성됩니다.

참고 keytool 유틸리티에 truststore 파일 암호를 생성할지 묻는 메시지가 나타날 수 있습니다. 나중에 truststore 파일에 추가 인증서를 추가할 경우 이 암호를 입력해야 합니다.

- 2 truststore 파일을 연결 서버 또는 보안 서버 호스트의 SSL 게이트웨이 구성 폴더에 복사하십시오.

예: `install_directory\VMware\VMware View\Server\ssl\gateway\conf\truststorefile.key`

다음에 수행할 작업

스마트 카드 인증을 사용하도록 설정하려면 연결 서버 구성 속성을 수정하십시오.

Horizon 연결 서버 구성 속성 수정

스마트 카드 인증을 사용하도록 설정하려면 연결 서버 또는 보안 서버 호스트에서 연결 서버 구성 속성을 수정해야 합니다.

사전 요구 사항

신뢰할 수 있는 모든 사용자 인증서에 대해 서버 truststore 파일에 CA(인증 기관) 인증서를 추가합니다. 이러한 인증서에는 루트 인증서가 포함되며, 사용자의 스마트 카드 인증서가 중간 인증 기관에서 발급된 경우에는 중간 인증서도 포함될 수 있습니다.

절차

- 1 연결 서버 또는 보안 서버 호스트의 TLS/SSL 게이트웨이 구성 폴더에 locked.properties 파일을 생성 또는 편집합니다.

예: `install_directory\VMware\VMware View\Server\ssl\gateway\conf\locked.properties`

- 2 trustKeyfile, trustStoretype, useCertAuth 속성을 locked.properties 파일에 추가하십시오.

a trustKeyfile을 truststore 파일 이름으로 설정하십시오.

b trustStoretype을 **jks**로 설정합니다.

c 인증서 인증을 사용하도록 설정하려면 useCertAuth를 **true**로 설정하십시오.

- 3 변경 내용을 적용하려면 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작합니다.

예제:locked.properties 파일

표시된 파일은 신뢰할 수 있는 모든 사용자에게 루트 인증서가 longq.key 파일에 위치하도록 지정하고 신뢰할 수 있는 저장 유형을 jks로 설정하며 인증서 인증을 사용하도록 설정합니다.

```
trustKeyfile=longq.key
trustStoretype=jks
useCertAuth=true
```

다음에 수행할 작업

연결 서버 인스턴스에 대해 스마트 카드 인증을 구성한 경우에는 Horizon Administrator에서 스마트 카드 인증 설정을 구성하십시오. 보안 서버에 대해서는 스마트 카드 인증 설정을 구성하지 않아도 됩니다. Horizon 연결 서버 인스턴스에 구성된 설정은 연결된 보안 서버에도 적용됩니다.

Horizon Administrator에서 스마트 카드 설정 구성

Horizon Administrator를 사용해 다른 스마트 카드 인증 시나리오를 수용하도록 설정할 수 있습니다.

연결 서버 인스턴스에서 이러한 설정을 구성하면 해당 설정이 연결된 보안 서버에도 적용됩니다.

사전 요구 사항

- 연결 서버 호스트에서 연결 서버 구성 속성을 수정하십시오.
- Horizon Client가 연결 서버 또는 보안 서버 호스트에 대해 직접 HTTPS 연결을 설정하는지 확인합니다. TLS 부하를 중간 디바이스로 분산하는 경우에는 스마트 카드 인증이 지원되지 않습니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 **연결 서버** 탭에서 연결 서버 인스턴스를 선택하고 **편집**을 클릭합니다.

3 원격 데스크톱 및 애플리케이션 사용자에게 대한 스마트 카드 인증을 구성하려면 다음 단계를 수행합니다.

- a 인증 탭의 View 인증 섹션에 있는 **사용자에게 대한 스마트 카드 인증** 드롭다운 메뉴에서 구성 옵션을 선택합니다.

옵션	조치
허용되지 않음	연결 서버 인스턴스에서 스마트 카드 인증을 사용할 수 없습니다.
선택 사항	사용자는 스마트 카드 인증 또는 암호 인증을 사용해 연결 서버 인스턴스에 연결할 수 있습니다. 스마트 카드 인증이 실패하면 사용자는 암호를 입력해야 합니다.
필수	<p>사용자는 연결 서버 인스턴스 연결 시 스마트 카드 인증을 사용해야 합니다. 스마트 카드 인증이 필요한 경우 사용자가 현재 사용자로 로그인 확인란을 선택하고 연결 서버 인스턴스에 연결하면 인증에 실패합니다. 이들 사용자는 연결 서버에 로그인할 때 스마트 카드와 PIN으로 재인증해야 합니다.</p> <p>참고 스마트 카드 인증은 Windows 암호 인증만 대체합니다. SecurID를 사용하도록 설정한 경우 사용자는 SecurID 및 스마트 카드 인증을 사용해 인증 받아야 합니다.</p>

- b 스마트 카드 제거 정책을 구성하십시오.

스마트 카드 인증을 **허용되지 않음**으로 설정한 경우 스마트 카드 제거 정책을 구성할 수 없습니다.

옵션	조치
사용자가 스마트 카드 제거 시 View 연결 서버에서 사용자 연결 끊기	스마트 카드 제거 시 사용자 세션 연결 해제 확인란을 선택합니다.
사용자가 스마트 카드 제거 시 View 연결 서버 연결을 유지하고 재인증 없이 새 데스크톱 또는 애플리케이션 세션 시작 허용	스마트 카드 제거 시 사용자 세션 연결 해제 확인란을 선택 해제하십시오.

사용자가 **현재 사용자로 로그인** 확인란을 선택하고 연결 서버 인스턴스에 연결하면 스마트 카드로 클라이언트 시스템에 로그인하더라도 스마트 카드 제거 정책이 적용되지 않습니다.

- c 스마트 카드 사용자 이름 힌트 기능을 구성하십시오.

스마트 카드 인증을 **허용되지 않음**으로 설정한 경우 스마트 카드 사용자 이름 힌트 기능을 구성할 수 없습니다.

옵션	조치
사용자가 단일 스마트 카드 인증서를 사용하여 여러 사용자 계정에 대해 인증하도록 설정	스마트 카드 사용자 이름 힌트 허용 확인란을 선택합니다.
사용자가 단일 스마트 카드 인증서를 사용하여 여러 사용자 계정에 대해 인증하도록 설정 안 함	스마트 카드 사용자 이름 힌트 허용 확인란을 선택 취소합니다.

- 4 Horizon Administrator에 로그인하는 관리자에 대한 스마트 카드 인증을 구성하려면 **인증** 탭을 클릭하고 View 관리 인증 섹션의 **관리자에 대한 스마트 카드 인증** 드롭다운 메뉴에서 구성 옵션을 선택합니다.

옵션	조치
허용되지 않음	연결 서버 인스턴스에서 스마트 카드 인증을 사용할 수 없습니다.
선택 사항	관리자가 스마트 카드 인증 또는 암호 인증을 사용하여 Horizon Administrator에 로그인할 수 있습니다. 스마트 카드 인증이 실패하면 관리자는 암호를 입력해야 합니다.
필수	관리자가 Horizon Administrator에 로그인할 때 스마트 카드 인증을 사용해야 합니다.

- 5 **확인**을 클릭합니다.

- 6 연결 서버 서비스를 다시 시작하십시오.

하나를 제외하고 스마트 설정 변경 사항을 적용하려면 연결 서버 서비스를 다시 시작해야 합니다. 연결 서버 서비스를 다시 시작하지 않고 **선택 사항**과 **필수** 간에 스마트 카드 인증 설정을 변경할 수 있습니다.

현재 로그인한 사용자와 관리자는 스마트 카드 설정 변경의 영향을 받지 않습니다.

다음에 수행할 작업

필요한 경우 스마트 카드 인증에 대한 Active Directory를 준비하십시오. [스마트 카드 인증을 위한 Active Directory 준비](#)의 내용을 참조하십시오.

스마트 카드 인증 구성을 확인하십시오. [스마트 카드 인증 구성 확인](#)의 내용을 참조하십시오.

타사 솔루션에서 스마트 카드 인증 구성

로드 밸런서 및 게이트웨이와 같은 타사 솔루션에서는 스마트 카드의 X.590 인증서와 암호화된 PIN이 포함된 SAML 어설션을 전달하여 스마트 카드 인증을 수행할 수 있습니다.

이 항목에서는 파트너 디바이스에서 인증서의 유효성을 검사한 후에 관련 X.590 인증서를 연결 서버에 제공하도록 타사 솔루션을 설정하는 것과 관련된 작업을 소개합니다. 이 기능에서는 SAML 인증을 사용하므로 Horizon Administrator에서 SAML 인증자를 생성하는 것도 작업에 포함됩니다.

Unified Access Gateway의 스마트 카드 인증 구성에 대한 자세한 내용은 Unified Access Gateway 배포 및 구성을 참조하십시오.

절차

- 타사 게이트웨이 또는 로드 밸런서에 대해 SAML 인증자를 생성합니다.
[Horizon Administrator에서 SAML 인증자 구성](#)의 내용을 참조하십시오.
- 원격 세션이 24시간 후에 종료되지 않도록 연결 서버 메타데이터의 만료 기간을 연장합니다.
[연결 서버에서 서비스 제공자 메타데이터의 만료 기간 변경](#)의 내용을 참조하십시오.
- 필요한 경우 타사 디바이스에서 연결 서버의 서비스 공급자 메타데이터를 사용하도록 구성합니다.
타사 디바이스의 제품 설명서를 참조하십시오.

4 타사 디바이스에 스마트 카드 설정을 구성합니다.

타사 디바이스의 제품 설명서를 참조하십시오.

스마트 카드 인증을 위한 Active Directory 준비

스마트 카드 인증을 구현할 때 Active Directory에서 특정 작업을 수행해야 할 수 있습니다.

■ 스마트 카드 사용자의 UPN 추가

스마트 카드 로그인에서 UPN(사용자 계정 이름)을 사용하기 때문에 스마트 카드를 사용해 Horizon 7에서 인증을 받는 사용자 및 관리자의 Active Directory 계정에 UPN이 올바르게 구성되어 있어야 합니다.

■ Enterprise NTAAuth 저장소에 루트 인증서 추가

CA를 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory의 Enterprise NTAAuth 저장소에 루트 인증서를 추가해야 합니다. Windows 도메인 컨트롤러를 루트 CA로 사용하면 이 절차를 수행할 필요가 없습니다.

■ 신뢰할 수 있는 루트 인증 기관에 루트 인증서 추가

인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory의 신뢰할 수 있는 루트 인증 기관 그룹 정책에 루트 인증서를 추가해야 합니다. Windows 도메인 컨트롤러를 루트 CA로 사용하면 이 절차를 수행할 필요가 없습니다.

■ 중간 인증 기관에 중간 인증서 추가

중간 인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory의 중간 인증 기관 그룹 정책에 중간 인증서를 추가해야 합니다.

스마트 카드 사용자의 UPN 추가

스마트 카드 로그인에서 UPN(사용자 계정 이름)을 사용하기 때문에 스마트 카드를 사용해 Horizon 7에서 인증을 받는 사용자 및 관리자의 Active Directory 계정에 UPN이 올바르게 구성되어 있어야 합니다.

스마트 카드 사용자가 위치한 도메인이 루트 인증서를 발급한 도메인과 다르면 사용자의 UPN을 신뢰할 수 있는 CA의 루트 인증서에 포함된 SAN(주체 대체 이름)으로 설정해야 합니다. 스마트 카드 사용자의 현재 도메인에 있는 서버에서 루트 인증서를 발급한 경우 사용자의 UPN을 수정할 필요가 없습니다.

참고 같은 도메인에서 인증서를 발급한 경우에도 기본 Active Directory 계정에 대한 UPN을 설정해야 할 수 있습니다. 관리자를 포함해 기본 계정에는 UPN이 기본적으로 설정되지 않습니다.

사전 요구 사항

- 인증서 속성을 확인해 신뢰할 수 있는 CA의 루트 인증서에 포함된 SAN을 가져오십시오.
- Active Directory 서버에 ADSI 편집 유틸리티가 없으면 Microsoft 웹 사이트에서 적절한 Windows 지원 도구를 다운로드하여 설치하십시오.

절차

- 1 Active Directory 서버에서 ADSI 편집 유틸리티를 시작하십시오.
- 2 왼쪽 창에서 사용자가 위치한 도메인을 확장하고 CN=Users를 두 번 클릭합니다.
- 3 오른쪽 창에서 마우스 오른쪽 단추로 사용자를 클릭한 다음 **속성**을 클릭합니다.
- 4 userPrincipalName 특성을 두 번 클릭하고 신뢰할 수 있는 CA 인증서의 SAN 값을 입력하십시오.
- 5 특성 설정을 저장하려면 **확인**을 클릭합니다.

Enterprise NTAUTH 저장소에 루트 인증서 추가

CA를 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory의 Enterprise NTAUTH 저장소에 루트 인증서를 추가해야 합니다. Windows 도메인 컨트롤러를 루트 CA로 사용하면 이 절차를 수행할 필요가 없습니다.

절차

- ◆ Enterprise NTAUTH 저장소에 인증서를 게시하려면 Active Directory 서버에서 certutil 명령을 사용하십시오.

예: `certutil -dspublish -f path_to_root_CA_cert NTAUTHCA`

이제 해당 CA에서 이러한 유형의 인증서를 신뢰하고 발급할 수 있습니다.

신뢰할 수 있는 루트 인증 기관에 루트 인증서 추가

인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory의 신뢰할 수 있는 루트 인증 기관 그룹 정책에 루트 인증서를 추가해야 합니다. Windows 도메인 컨트롤러를 루트 CA로 사용하면 이 절차를 수행할 필요가 없습니다.

절차

- 1 Active Directory 서버에서 그룹 정책 관리 플러그인으로 이동하십시오.

AD 버전	탐색 경로
Windows 2003	<ol style="list-style-type: none"> a 시작 > 모든 프로그램 > 관리 도구 > Active Directory 사용자 및 컴퓨터를 선택합니다. b 도메인을 마우스 오른쪽 단추로 클릭하고 속성을 클릭합니다. c 그룹 정책 탭에서 열기를 클릭하여 그룹 정책 관리 플러그인을 엽니다. d 기본 도메인 정책을 마우스 오른쪽 단추로 클릭하고 편집을 클릭합니다.
Windows 2008	<ol style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.

AD 버전	탐색 경로
Windows 2012 R2	<ul style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.
Windows 2016	<ul style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.

- 2 컴퓨터 구성 섹션을 확장하고 **Windows 설정\보안 설정\공개 키**를 여십시오.
- 3 신뢰할 수 있는 루트 인증 기관을 마우스 오른쪽 버튼으로 클릭하고 **가져오기**를 선택합니다.
- 4 마법사에 표시된 메시지에 따라 루트 인증서(예: rootCA.cer)를 가져오고 **확인**을 클릭합니다.
- 5 그룹 정책 창을 닫습니다.

이제 도메인의 모든 시스템에서 신뢰할 수 있는 루트 저장소의 루트 인증서 복사본을 가지고 있습니다.

다음에 수행할 작업

중간 인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory의 중간 인증 기관 그룹 정책에 중간 인증서를 추가하십시오. [중간 인증 기관에 중간 인증서 추가](#)의 내용을 참조하십시오.

중간 인증 기관에 중간 인증서 추가

중간 인증 기관(CA)을 사용해 스마트 카드 로그인 또는 도메인 컨트롤러 인증서를 발급하는 경우 Active Directory의 중간 인증 기관 그룹 정책에 중간 인증서를 추가해야 합니다.

절차

- 1 Active Directory 서버에서 그룹 정책 관리 플러그인으로 이동하십시오.

AD 버전	탐색 경로
Windows 2003	<ul style="list-style-type: none"> a 시작 > 모든 프로그램 > 관리 도구 > Active Directory 사용자 및 컴퓨터를 선택합니다. b 도메인을 마우스 오른쪽 단추로 클릭하고 속성을 클릭합니다. c 그룹 정책 탭에서 열기를 클릭하여 그룹 정책 관리 플러그인을 엽니다. d 기본 도메인 정책을 마우스 오른쪽 단추로 클릭하고 편집을 클릭합니다.
Windows 2008	<ul style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.
Windows 2012 R2	<ul style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.
Windows 2016	<ul style="list-style-type: none"> a 시작 > 관리 도구 > 그룹 정책 관리를 선택합니다. b 도메인을 확장하고 기본 도메인 정책을 마우스 오른쪽 버튼으로 클릭하고 편집을 클릭합니다.

- 2 컴퓨터 구성 섹션을 확장하고 **Windows 설정\보안 설정\공개 키**에 대한 정책을 엽니다.

- 3 **중간 인증 기관**을 마우스 오른쪽 버튼으로 클릭하고 **가져오기**를 선택합니다.
- 4 마법사에 표시된 메시지에 따라 중간 인증서(예: intermediateCA.cer)를 가져오고 **확인**을 클릭합니다.
- 5 그룹 정책 창을 닫습니다.

이제 도메인의 모든 시스템에서 중간 인증 기관 저장소의 중간 인증서 복사본을 가지고 있습니다.

스마트 카드 인증 구성 확인

처음으로 스마트 카드 인증을 설정하고 나서 또는 스마트 카드 인증이 올바르게 작동하지 않을 경우 스마트 카드 인증 구성을 확인해야 합니다.

절차

- 각 클라이언트 시스템에 스마트 카드 미들웨어, 유효한 인증서를 가진 스마트 카드 및 스마트 카드 판독기가 있는지 확인합니다. 최종 사용자의 경우 Horizon Client가 있는지 확인합니다.
스마트 카드 소프트웨어 및 하드웨어 구성에 대한 자세한 내용은 스마트 카드 공급업체에서 제공한 설명서를 참조하십시오.
- 각 클라이언트 시스템에서 **시작 > 설정 > 제어판 > 인터넷 옵션 > 내용 > 인증서 > 개인**을 선택하여 스마트 카드 인증에 필요한 인증서가 있는지 확인합니다.
사용자나 관리자가 스마트 카드 판독기에 스마트 카드를 삽입하면 Windows가 스마트 카드에서 사용자의 컴퓨터로 인증서를 복사합니다. 이러한 인증서는 Horizon Client를 포함한 클라이언트 시스템에 있는 애플리케이션에서 사용할 수 있습니다.
- 연결 서버 또는 보안 서버 호스트의 `locked.properties` 파일에서 `useCertAuth` 속성이 **true**로 설정되어 있고 절차가 올바른지 확인합니다.
`locked.properties` 파일은 `install_directory\VMware\VMware View\Server\Wsslgateway\conf`에 있습니다. `useCertAuth` 속성은 대개 철자가 `userCertAuth`로 잘못되어 있습니다.
- 연결 서버 인스턴스에 스마트 카드 인증을 구성한 경우 Horizon Administrator에서 스마트 카드 인증 설정을 확인하십시오.
 - a **View 구성 > 서버**를 선택합니다.
 - b **연결 서버** 탭에서 연결 서버 인스턴스를 선택하고 **편집**을 클릭합니다.
 - c 사용자에게 대해 스마트 카드 인증을 구성한 경우에는 **인증** 탭에서 **사용자에게 대한 스마트 카드 인증이 선택 사항** 또는 **필수**로 설정되었는지 확인합니다.
 - d 관리자에게 대해 스마트 카드 인증을 구성한 경우에는 **인증** 탭에서 **관리자에게 대한 스마트 카드 인증이 선택 사항** 또는 **필수**로 설정되었는지 확인합니다.
 스마트 카드 설정에 변경 사항을 적용하려면 연결 서버 서비스를 다시 시작해야 합니다.

- 스마트 카드 사용자가 있는 도메인이 루트 인증서가 발행된 도메인과 다른 경우, 사용자의 UPN이 신뢰된 CA의 루트 인증서에 포함된 SAN으로 설정되어 있는지 확인합니다.
 - a 인증서 속성을 보고 신뢰된 CA의 루트 인증서에 포함된 SAN을 찾으십시오.
 - b Active Directory 서버에서 **시작 > 관리 도구 > Active Directory 사용자 및 컴퓨터**를 선택합니다.
 - c **사용자** 폴더에서 사용자를 마우스 오른쪽 단추로 클릭하고 **속성**을 선택합니다.
 계정 탭의 **사용자 로그인 이름** 텍스트 상자에 UPN이 표시됩니다.
- 스마트 카드 사용자가 PCoIP 디스플레이 프로토콜이나 VMware Blast 디스플레이 프로토콜을 선택하여 단일 세션 데스크톱에 연결할 경우에는 단일 사용자 시스템에 스마트 카드 리디렉션이라는 View Agent 또는 Horizon Agent 구성 요소가 설치되어 있는지 확인합니다. 스마트 카드 기능을 이용하면 사용자가 스마트 카드를 사용해서 단일 세션 데스크톱에 로그인할 수 있습니다. 원격 데스크톱 서비스 역할이 설치된 RDS 호스트는 스마트 카드 기능을 자동으로 지원하므로 해당 기능을 설치할 필요가 없습니다.
- 스마트 카드 인증을 사용하도록 설정되었다는 메시지를 보려면 연결 서버 또는 보안 서버 호스트의 `drive:W\Documents and Settings\All Users\Application Data\VMware\WDM\logs`에서 로그 파일을 확인하십시오.

스마트 카드 인증서 해지 검사 사용

인증서 해지 확인을 구성하여 사용자 인증서를 해지한 사용자가 스마트 카드를 사용하여 인증하지 못하도록 할 수 있습니다. 인증서는 사용자가 조직을 떠나거나 스마트 카드를 분실하거나 부서를 다른 부서로 이동할 경우 해지되기도 합니다.

Horizon 7에서는 인증서 해지 목록(CRL) 및 온라인 인증서 상태 프로토콜(OCSP)을 사용하여 인증서 해지 확인을 지원합니다. CRL은 인증서를 발행한 CA에서 게시한 해지된 인증서 목록입니다. OCSP는 X.509 인증서의 해지 상태를 얻는 데 사용되는 인증서 유효성 검사 프로토콜입니다.

연결 서버 인스턴스 또는 보안 서버에서 인증서 해지 확인을 구성할 수 있습니다. 연결 서버 인스턴스가 보안 서버와 연결될 때 보안 서버에서 인증서 해지 확인을 구성할 수 있습니다. CA는 연결 서버 인스턴스 또는 보안 서버 호스트에서 액세스할 수 있어야 합니다.

동일한 연결 서버 인스턴스 또는 보안 서버에서 CRL 및 OCSP 모두를 구성할 수 있습니다. 인증서 해지 확인의 두 가지 유형 모두를 구성할 경우, Horizon 7에서 OCSP를 먼저 사용하려고 하며 OCSP가 실패할 경우 CRL로 변경합니다. CRL이 실패해도 Horizon 7에서는 OCSP로 변경하지 않습니다.

■ CRL 검사를 사용하여 로그인

CRL 검사를 구성하면 Horizon 7에서 CRL을 구성하고 읽어 사용자 인증서의 해지 상태를 결정합니다.

■ OCSP 인증서 해지 검사를 사용하여 로그인

OCSP 인증서 해지 검사를 구성하면 Horizon 7에서 OCSP 응답자에 확인 요청을 보내 특정 사용자 인증서의 해지 상태를 결정합니다. Horizon 7에서는 OCSP 서명 인증서를 사용해 OCSP 응답자로부터 받은 응답이 진짜인지 확인합니다.

■ CRL 검사 구성

CRL 검사를 구성하면 Horizon 7에서 CRL을 읽고 스마트 카드 사용자 인증서의 해지 상태를 결정합니다.

■ OCSP 인증서 해지 검사 구성

OCSP 인증서 해지 검사를 구성하면 Horizon 7에서 OCSP 응답자에 확인 요청을 보내 스마트 카드 사용자 인증서 해지 상태를 결정합니다.

■ 스마트 카드 인증서 해지 검사 속성

locked.properties 파일에서 값을 설정하여 스마트 카드 인증서 해지 확인을 사용하도록 설정하고 구성합니다.

CRL 검사를 사용하여 로그인

CRL 검사를 구성하면 Horizon 7에서 CRL을 구성하고 읽어 사용자 인증서의 해지 상태를 결정합니다.

인증서를 해지하고 스마트 카드 인증이 선택 사항인 경우 **사용자 이름 및 암호를 입력하십시오** 대화 상자가 나타나고 사용자가 인증을 받으려면 암호를 입력해야 합니다. 스마트 카드로 인증이 필요한 경우에는 오류 메시지가 표시되고 인증을 받을 수 없습니다. Horizon 7에서 CRL을 읽을 수 없을 때도 동일한 이벤트가 발생합니다.

OCSP 인증서 해지 검사를 사용하여 로그인

OCSP 인증서 해지 검사를 구성하면 Horizon 7에서 OCSP 응답자에 확인 요청을 보내 특정 사용자 인증서의 해지 상태를 결정합니다. Horizon 7에서는 OCSP 서명 인증서를 사용해 OCSP 응답자로부터 받은 응답이 진짜인지 확인합니다.

사용자가 인증서를 해지하고 스마트 카드 인증이 선택 사항인 경우 **사용자 이름 및 암호를 입력하십시오** 대화 상자가 나타나고 사용자가 인증을 받으려면 암호를 입력해야 합니다. 스마트 카드로 인증이 필요한 경우에는 오류 메시지가 표시되고 인증을 받을 수 없습니다.

Horizon 7에서는 OCSP 응답자로부터 응답을 받지 못하거나 응답이 잘못된 경우 CRL 검사로 변경합니다.

CRL 검사 구성

CRL 검사를 구성하면 Horizon 7에서 CRL을 읽고 스마트 카드 사용자 인증서의 해지 상태를 결정합니다.

사전 요구 사항

CRL 검사에 대한 locked.properties 파일 속성을 숙지하십시오. **스마트 카드 인증서 해지 검사 속성**의 내용을 참조하십시오.

절차

- 1 연결 서버 또는 보안 서버 호스트의 TLS/SSL 게이트웨이 구성 폴더에 `locked.properties` 파일을 생성 또는 편집합니다.

예: `install_directory\VMware\VMware View\Server\ssl\gateway\conf\locked.properties`

- 2 `enableRevocationChecking` 및 `crllLocation` 속성을 `locked.properties` 파일에 추가하십시오.
 - a 스마트 카드 인증서 해지 검사를 사용하도록 설정하려면 `enableRevocationChecking`을 **true**로 설정하십시오.
 - b `crllLocation`을 CRL 위치로 설정하십시오. 해당 값이 URL 또는 파일 경로가 될 수 있습니다.
- 3 변경 내용을 적용하려면 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작합니다.

예제:locked.properties 파일

표시된 파일은 스마트 카드 인증 및 스마트 카드 인증서 해지 검사를 사용하도록 설정하고 CRL 검사를 구성하며 CRL 위치에 대한 URL을 지정할 수 있습니다.

```
trustKeyfile=longa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
crllLocation=http://root.ocsp.net/certEnroll/ocsp-ROOT_CA.crl
```

OCSP 인증서 해지 검사 구성

OCSP 인증서 해지 검사를 구성하면 Horizon 7에서 OCSP 응답자에 확인 요청을 보내 스마트 카드 사용자 인증서 해지 상태를 결정합니다.

사전 요구 사항

OCSP 인증서 해지 검사에 대한 `locked.properties` 파일 속성을 숙지하십시오. [스마트 카드 인증서 해지 검사 속성](#)의 내용을 참조하십시오.

절차

- 1 연결 서버 또는 보안 서버 호스트의 TLS/SSL 게이트웨이 구성 폴더에 `locked.properties` 파일을 생성 또는 편집합니다.

예: `install_directory\VMware\VMware View\Server\ssl\gateway\conf\locked.properties`
- 2 `locked.properties` 파일에 `enableRevocationChecking`, `enableOCSP`, `ocspURL` 및 `ocspSigningCert` 속성을 추가합니다.
 - a 스마트 카드 인증서 해지 검사를 사용하도록 설정하려면 `enableRevocationChecking`을 **true**로 설정하십시오.
 - b OCSP 인증서 해지 검사를 사용하려면 `enableOCSP`를 **true**로 설정하십시오.
 - c `ocspURL`을 OCSP 응답자의 URL로 설정하십시오.
 - d `ocspSigningCert`를 OCSP 응답자의 서명 인증서를 포함하는 파일 위치로 설정하십시오.

3 변경 내용을 적용하려면 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작합니다.

예제:locked.properties 파일

표시된 파일은 스마트 카드 인증 및 스마트 카드 인증서 해지 검사를 사용하도록 설정하고 CRL과 OCSP 인증서 해지 검사를 구성하며 OCSP 응답자 위치를 지정하고 OCSP 서명 인증서를 포함하는 파일을 확인할 수 있습니다.

```
trustKeyfile=lonqa.key
trustStoretype=jks
useCertAuth=true
enableRevocationChecking=true
enableOCSP=true
allowCertCRLs=true
ocspSigningCert=te-ca.signing.cer
ocspURL=http://te-ca.lonqa.int/ocsp
```

스마트 카드 인증서 해지 검사 속성

locked.properties 파일에서 값을 설정하여 스마트 카드 인증서 해지 확인을 사용하도록 설정하고 구성합니다.

[표3-1](#)에는 인증서 해지 확인을 위한 locked.properties 파일 속성이 나열됩니다.

표 3-1. 스마트 카드 인증서 해지 검사 속성

속성	설명
enableRevocationChecking	이 속성을 true 로 설정하여 인증서 해지 확인을 사용하도록 설정합니다. 이 속성이 false 로 설정된 경우 인증서 해지 확인이 사용되지 않도록 설정되고 다른 모든 인증서 해지 확인 속성이 무시됩니다. 기본값은 false 입니다.
cr lLocat ion	CRL 위치(URL 또는 파일 경로일 수 있음)를 지정합니다. URL을 지정하지 않거나 지정된 URL이 잘못된 경우 Horizon 7에서는 allowCertCRLs가 true 로 설정되었거나 지정되지 않았을 때 사용자 인증서의 CRL 목록을 사용합니다. Horizon 7에서 CRL에 액세스할 수 없는 경우 CRL 확인에 실패합니다.
al lowCer tCRLs	이 속성이 true 로 설정된 경우 Horizon 7은 사용자 인증서에서 CRL 목록을 추출합니다. 기본값은 true 입니다.
enableOCSP	이 속성을 true 로 설정하여 OCSP 인증서 해지 확인을 사용하도록 설정합니다. 기본값은 false 입니다.
ocspURL	OCSP 응답자의 URL을 지정합니다.
ocspResponderCer t	OCSP 응답자의 서명 인증서가 포함된 파일을 지정합니다. Horizon 7에서는 이 인증서를 사용하여 OCSP 응답자의 응답이 정품인지 확인합니다.

표 3-1. 스마트 카드 인증서 해지 검사 속성 (계속)

속성	설명
ocspSendNonce	이 속성이 true 로 설정되면 OCSP 요청을 사용하여 nonce를 보내 응답이 반복되지 않도록 합니다. 기본값은 false 입니다.
ocspCRLFailover	이 속성이 true 로 설정되면 Horizon 7에서는 OCSP 인증서 해지 확인이 실패할 경우 CRL 확인을 사용합니다. 기본값은 true 입니다.

다른 유형의 사용자 인증 설정

Horizon 7는 기존 Active Directory 인프라를 사용하여 사용자와 관리자를 인증하고 관리합니다. 스마트 카드 외에도 생체 인식 인증이나 RSA SecurID 및 RADIUS와 같은 2 요소 인증 솔루션과 같은 다른 인증 방식을 Horizon 7에 통합하여 원격 데스크톱 및 애플리케이션 사용자를 인증할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 2 요소 인증 사용
- SAML 인증 사용
- 생체 인식 인증 구성

2 요소 인증 사용

사용자가 RSA SecurID 인증 또는 RADIUS(Remote Authentication Dial-In User Service) 인증을 사용해야만 하도록 Horizon 연결 서버 인스턴스를 구성할 수 있습니다.

- RADIUS 지원은 다양한 대체 2 요소 토큰 기반 인증 옵션을 제공합니다.
- 또한 Horizon 7는 타사 솔루션 공급자가 고급 인증 확장을 Horizon 7에 통합할 수 있는 개방형 표준 확장 인터페이스를 제공합니다.

RSA SecurID 및 RADIUS와 같은 2 요소 인증 솔루션은 별도의 서버에 설치되어 인증 관리자와 함께 작동하므로 그러한 서버가 연결 서버 호스트에 액세스할 수 있도록 구성해야 합니다. 예를 들어, RSA SecurID를 사용할 경우 인증 관리자는 RSA 인증 관리자가 됩니다. RADIUS를 사용할 경우 인증 관리자는 RADIUS 서버가 됩니다.

2 요소 인증을 사용하려면 각 사용자에게 인증 관리자에 등록된 RSA SecurID 토큰과 같은 토큰이 있어야 합니다. 2 요소 인증 토큰은 고정 간격으로 인증 코드를 생성하는 하드웨어 또는 소프트웨어의 일부입니다. 보통 인증을 수행하려면 PIN과 인증 코드를 알아야 합니다.

여러 연결 서버 인스턴스가 있는 경우, 일부 인스턴스에 2 요소 인증을 구성하고 나머지는 다른 사용자 인증 방법을 구성할 수 있습니다. 예를 들어 인터넷을 통해 회사 네트워크 외부에서 원격 데스크톱 및 애플리케이션에 액세스하는 사용자 전용으로 2 요소 인증을 구성할 수 있습니다.

Horizon 7는 RSA SecurID 준비 프로그램을 통해 인증되며 새 PIN 모드, 다음 토큰 코드 모드, RSA 인증 관리자 및 로드 밸런싱을 포함하여 SecurID 기능의 전 범위를 지원합니다.

■ 2 요소 인증을 사용한 로그인

사용자가 RSA SecurID 인증 또는 RADIUS 인증을 사용하도록 설정할 수 있는 연결 서버 인스턴스에 연결하면 Horizon Client에 특별한 로그인 대화 상자가 나타납니다.

■ Horizon Administrator에서 2 요소 인증 사용

Horizon Administrator에서 연결 서버 설정을 수정하여 RSA SecurID 인증 또는 RADIUS 인증을 사용하도록 연결 서버 인스턴스를 설정할 수 있습니다.

■ RSA SecurID 액세스 거부 문제 해결

Horizon Client가 RSA SecurID 인증을 사용하여 연결할 때 액세스가 거부됩니다.

■ RADIUS 액세스 거부 문제 해결

Horizon Client가 RADIUS 2 요소 인증을 사용하여 연결하면 액세스가 거부됩니다.

2 요소 인증을 사용한 로그인

사용자가 RSA SecurID 인증 또는 RADIUS 인증을 사용하도록 설정할 수 있는 연결 서버 인스턴스에 연결하면 Horizon Client에 특별한 로그인 대화 상자가 나타납니다.

사용자는 이 특별한 로그인 대화 상자에 자신의 RSA SecurID 인증 또는 RADIUS 인증 사용자 이름과 암호를 입력해야 합니다. 2 요소 인증 암호는 대개 PIN과 그 다음에 나오는 토큰 코드로 구성됩니다.

- 사용자가 RSA SecurID 사용자 이름 및 암호를 입력한 후에 RSA 인증 관리자에서 새 RSA SecurID PIN을 요청하면 PIN 대화 상자가 나타납니다. 새 PIN을 설정하면 로그인하기 전에 다음 토큰 코드를 기다리라는 메시지가 표시됩니다. RSA 인증 관리자에서 시스템 생성 PIN을 사용하도록 구성한 경우에는 PIN을 확인하는 대화 상자가 나타납니다.

- Horizon 7 로그인 시 RADIUS 인증은 RSA SecurID 인증과 유사한 방식으로 작동합니다. RADIUS 서버가 액세스 챌린지를 생성하면 Horizon Client는 다음 토큰 코드를 묻는 RSA SecurID 메시지와 유사한 대화 상자를 표시합니다. 현재 RADIUS 챌린지에는 텍스트 입력을 요구하는 메시지만 지원됩니다. RADIUS 서버에서 보낸 모든 챌린지 텍스트는 표시되지 않습니다. 다중 선택 및 이미지 선택같이 복잡한 챌린지 유형은 아직 지원되지 않습니다.

사용자가 Horizon Client에 자격 증명을 입력하면 RADIUS 서버는 SMS 텍스트 메시지나 이메일 또는 다른 대역 외 메커니즘을 이용하는 텍스트를 코드와 함께 사용자의 휴대 전화로 전송할 수 있습니다. 사용자가 이 텍스트와 코드를 Horizon Client에 입력하면 인증이 완료됩니다.

- 일부 RADIUS 벤더는 Active Directory에서 사용자를 가져오는 기능을 제공하기 때문에 경우에 따라서는 RADIUS 인증 사용자 이름과 암호를 묻기 전에 Active Directory 자격 증명을 묻는 메시지에서 표시될 수 있습니다.

Horizon Administrator에서 2 요소 인증 사용

Horizon Administrator에서 연결 서버 설정을 수정하여 RSA SecurID 인증 또는 RADIUS 인증을 사용하도록 연결 서버 인스턴스를 설정할 수 있습니다.

사전 요구 사항

인증 관리 서버에 RSA SecurID 소프트웨어 또는 RADIUS 소프트웨어 같은 2 요소 인증 소프트웨어를 설치하고 구성합니다.

- RSA SecurID 인증의 경우 연결 서버 인스턴스에 사용할 `sdconf.rec` 파일을 RSA 인증 관리자에게서 내보냅니다. RSA 인증 관리자 설명서를 참조하십시오.
- RADIUS 인증의 경우, 벤더의 구성 설명서를 참조하십시오. RADIUS 서버의 호스트 이름이나 IP 주소, RADIUS 인증을 수신하는 포트 번호(대개 1812), 인증 유형(PAP, CHAP, MS-CHAPv1 또는 MS-CHAPv2) 및 공유 암호를 기록해 둡니다. 이러한 값을 Horizon Administrator에 입력해야 합니다. 기본 및 보조 RADIUS 인증자에 대해 값을 입력할 수 있습니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 **연결 서버** 탭에서 서버를 선택하고 **편집**을 클릭합니다.
- 3 **인증** 탭의 고급 인증 섹션에 있는 **2 요소 인증** 드롭다운 목록에서 **RSA SecureID** 또는 **RADIUS**를 선택합니다.
- 4 RSA SecurID 또는 RADIUS 사용자 이름과 Active Directory의 사용자 이름이 일치하도록 맞추려면 **일치하는 SecurID 및 Windows 사용자 이름 적용** 또는 **2 요소 및 Windows 사용자 이름 일치 강제 적용**을 선택합니다.

이 옵션을 선택한 경우 사용자는 Active Directory 인증에 대해 동일한 RSA SecurID 또는 RADIUS 사용자 이름을 사용해야 합니다. 이 옵션을 선택하지 않으면 이름이 다를 수 있습니다.

- 5 RSA SecurID의 경우 **파일 업로드**를 클릭하고 `sdconf.rec` 파일의 위치를 입력하거나 **찾아보기**를 클릭하여 파일을 검색합니다.

6 RADIUS 인증에 필요한 다음의 나머지 필드를 모두 지정합니다.

- a 토큰 코드의 대역 외 전송을 트리거하는 Windows 인증이 초기 RADIUS 인증에 사용되며 이 토큰 코드가 RADIUS 챌린지의 일부인 경우에는 **RADIUS 및 Windows 인증에 대해 동일한 사용자 이름 및 암호 사용**을 선택합니다.

이 확인란을 선택하면 RADIUS 인증에 Windows 사용자 이름과 암호를 사용할 경우 RADIUS 인증이 완료된 이후에 Windows 자격 증명을 묻는 메시지가 표시되지 않습니다. 따라서 RADIUS 인증 후에 사용자가 Windows 사용자 이름과 암호를 다시 입력할 필요가 없습니다.

- b **인증자** 드롭다운 목록에서 **새 인증자 생성**을 선택한 후 페이지를 완료합니다.

- RADIUS 계정을 사용하려는 경우가 아니면 **계정 포트**를 **0**으로 설정합니다. RADIUS 서버가 계정 데이터를 수집할 수 있는 경우에만 이 포트를 0이 아닌 숫자로 설정하십시오. RADIUS 서버가 계정 메시지를 지원하지 않는 경우에 이 포트를 0이 아닌 숫자로 설정하면 메시지가 전송되고 무시되는 과정이 여러 번 반복되어 인증이 지연될 수 있습니다.

계정 데이터는 사용 시간 및 사용 데이터를 기준으로 사용자에게 비용을 청구하는 데 사용될 수 있습니다. 계정 데이터는 일반적인 네트워크 모니터링 및 통계 용도로도 사용될 수 있습니다.

- 영역 접두사 문자열을 지정하면 RADIUS 서버로 보내는 사용자 이름 앞에 해당 문자열이 추가됩니다. 예를 들어, Horizon Client에 입력한 이름이 **jdoo**이고, 지정한 영역 접두사가 **DOMAIN-AW**이면 **DOMAIN-AWjdoo**라는 사용자 이름이 RADIUS 서버에 전송됩니다. 마찬가지로, **@mycorp.com**이라는 문자열을 영역 접미사로 사용하면 **jdoo@mycorp.com**이라는 사용자 이름이 RADIUS 서버에 전송됩니다.

7 변경 사항을 저장하려면 **확인**을 클릭합니다.

연결 서버 서비스를 다시 시작하지 않아도 됩니다. 필요한 구성 파일이 자동으로 배포되고 구성 설정이 즉시 적용됩니다.

사용자가 Horizon Client를 열고 연결 서버에 인증되면 2 요소 인증 메시지가 표시됩니다. RADIUS 인증을 사용하는 경우 지정한 토큰 레이블이 포함된 텍스트 메시지가 로그인 대화상자에 표시됩니다.

RADIUS 인증 설정에 대한 변경 사항은 구성을 변경한 이후에 시작한 원격 데스크톱 및 애플리케이션 세션에 영향을 줍니다. 현재 세션에는 RADIUS 인증 설정 변경 내용이 영향을 주지 않습니다.

다음에 수행할 작업

연결 서버 인스턴스의 복제된 그룹이 있고 이러한 인스턴스에 RADIUS 인증도 설정하려는 경우 기존 RADIUS 인증자 구성을 다시 사용할 수 있습니다.

RSA SecurID 액세스 거부 문제 해결

Horizon Client가 RSA SecurID 인증을 사용하여 연결할 때 액세스가 거부됩니다.

문제

RSA SecurID를 사용하여 Horizon Client 연결을 설정하면 액세스가 거부됨이 표시되고 RSA 인증 관리자 로그 모니터에 노드 확인이 실패함 오류가 표시됩니다.

원인

RSA Agent 호스트 노드 비밀을 재설정해야 합니다.

해결책

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 **연결 서버** 탭에서 연결 서버를 선택하고 **편집**을 클릭합니다.
- 3 **인증** 탭에서 **노드 암호 지우기**를 선택합니다.
- 4 노드 비밀을 지우려면 **확인**을 클릭합니다.
- 5 RSA 인증 관리자를 실행 중인 컴퓨터에서 **시작 > 프로그램 > RSA 보안 > RSA 인증 관리자 호스트 모드**를 선택합니다.
- 6 **에이전트 호스트 > 에이전트 호스트 편집**을 선택합니다.
- 7 목록에서 **View 연결 서버**를 선택하고 **노드 비밀 생성** 확인란 선택을 해제합니다.
편집할 때마다 기본적으로 **노드 암호 생성**이 선택됩니다.
- 8 **확인**을 클릭합니다.

RADIUS 액세스 거부 문제 해결

Horizon Client가 RADIUS 2 요소 인증을 사용하여 연결하면 액세스가 거부됩니다.

문제

RADIUS 2 요소 인증을 사용하는 Horizon Client 연결에 대해 액세스가 거부됨이 표시됩니다.

원인

RADIUS가 RADIUS 서버의 응답을 받지 못하여 Horizon 7 시간 초과가 발생합니다.

해결책

이 문제는 다음과 같은 일반적인 구성 실수 때문에 발생합니다.

- 연결 서버 인스턴스를 RADIUS 클라이언트로 허용하도록 RADIUS 서버를 구성하지 않았습니다.
RADIUS를 사용하는 각 연결 서버 인스턴스를 RADIUS 서버에 클라이언트로 설정해야 합니다.
사용 중인 RADIUS 2 요소 인증 제품에 대한 설명서를 참조하십시오.
- 연결 서버 인스턴스와 RADIUS 서버의 공유 암호 값이 일치하지 않습니다.

SAML 인증 사용

SAML(Security Assertion Markup Language)은 여러 보안 도메인 간에 인증 및 권한 부여 정보를 설명하고 교환하는 데 사용되는 XML 기반 표준입니다. SAML은 SAML 어설션이라는 XML 문서로 ID 공급자와 서비스 공급자 간에 사용자 정보를 전달합니다.

SAML 인증을 사용하여 Horizon 7을 VMware Workspace ONE, VMware Identity Manager 또는 자격 있는 타사 로드 밸런서나 게이트웨이와 통합할 수 있습니다. 타사 디바이스에 대해 SAML을 구성할 경우 SAML을 사용하도록 Horizon 7을 구성하는 방법에 대한 내용은 벤더 설명서를 참조하십시오. SSO를 사용하도록 설정된 경우 VMware Identity Manager 또는 타사 디바이스에 로그인한 사용자는 두 번째 로그인 절차를 거치지 않고도 원격 데스크톱 및 애플리케이션을 시작할 수 있습니다. SAML 인증을 사용하여 VMware Access Point나 타사 디바이스에 스마트 카드 인증을 구현할 수도 있습니다.

인증 권한을 Workspace ONE, VMware Identity Manager 또는 타사 디바이스에 위임하려면 Horizon 7에서 SAML 인증자를 생성해야 합니다. SAML 인증자에는 Horizon 7과 Workspace ONE, VMware Identity Manager 또는 View와 타사 디바이스 간의 신뢰 및 메타데이터 교환이 포함되어 있습니다. SAML 인증자와 연결 서버 인스턴스를 연결해야 합니다.

VMware Identity Manager 통합을 위해 SAML 인증 사용

Horizon 7과 VMware Identity Manager(이전 이름은 Workspace ONE) 사이의 통합에서는 SAML 2.0 표준을 사용하여 SSO(Single Sign-On) 기능에 필수적인 상호 신뢰를 형성합니다. SSO를 사용하도록 설정된 경우 Active Directory 자격 증명으로 VMware Identity Manager 또는 Workspace ONE에 로그인한 사용자는 두 번째 로그인 절차를 거치지 않고도 원격 데스크톱 및 애플리케이션을 시작할 수 있습니다.

VMware Identity Manager와 Horizon 7가 통합된 경우 VMware Identity Manager는 사용자가 VMware Identity Manager에 로그인하여 데스크톱 또는 애플리케이션 아이콘을 클릭할 때마다 고유한 SAML 아티팩트를 생성합니다. VMware Identity Manager는 이 SAML 아티팩트를 사용하여 URI(Universal Resource Identifier)를 생성합니다. URI에는 데스크톱 또는 애플리케이션 풀이 상주하는 연결 서버 인스턴스, 시작할 데스크톱 또는 애플리케이션, SAML 아티팩트 등에 대한 정보가 포함됩니다.

VMware Identity Manager가 SAML 아티팩트를 Horizon Client에 보내면 Horizon Client가 해당 아티팩트를 연결 서버 인스턴스에 보냅니다. 그런 다음 연결 서버 인스턴스가 SAML 아티팩트를 사용하여 VMware Identity Manager에서 SAML 어설션을 검색합니다.

SAML 어설선이 수신되면 연결 서버 인스턴스가 어설션을 검증하고 사용자의 암호를 해독한 다음 해독된 암호를 사용하여 데스크톱 또는 애플리케이션을 시작합니다.

VMware Identity Manager 및 Horizon 7 통합 설정 과정에는 Horizon 7 정보로 VMware Identity Manager를 구성하는 단계와 인증 책임을 VMware Identity Manager에 위임하도록 Horizon 7을 구성하는 단계가 포함됩니다.

인증 책임을 VMware Identity Manager에 위임하려면 Horizon 7에서 SAML 인증자를 생성해야 합니다. SAML 인증자에는 Horizon 7과 VMware Identity Manager 간의 신뢰 및 메타데이터 교환이 포함됩니다. SAML 인증자와 연결 서버 인스턴스를 연결해야 합니다.

참고 VMware Identity Manager를 통해 데스크톱 및 애플리케이션에 대한 액세스를 제공하려는 경우 Horizon Administrator에서 루트 액세스 그룹에 대한 관리자 역할을 가진 사용자로 데스크톱 및 애플리케이션 풀을 생성하는지 확인해야 합니다. 사용자에게 루트 액세스 그룹이 아닌 다른 액세스 그룹에 대한 관리자 역할을 부여할 경우 VMware Identity Manager가 Horizon 7에 구성된 SAML 인증자를 인식하지 못하므로 VMware Identity Manager에 풀을 구성할 수 없습니다.

Horizon Administrator에서 SAML 인증자 구성

VMware Identity Manager에서 원격 데스크톱 및 애플리케이션을 실행하거나 타사 로드 밸런서 또는 게이트웨이를 통해 원격 데스크톱 및 애플리케이션에 연결하려면 Horizon Administrator에서 SAML 인증자를 생성해야 합니다. SAML 인증자에는 Horizon 7와 클라이언트에서 연결하는 디바이스 간의 신뢰 및 메타데이터 교환이 포함되어 있습니다.

SAML 인증자와 연결 서버 인스턴스를 연결해야 합니다. 배포에 둘 이상의 연결 서버 인스턴스가 포함된 경우 SAML 인증자를 각 인스턴스에 연결해야 합니다.

한 번에 하나의 고정 인증자와 여러 개의 동적 인증자를 실행하도록 허용할 수 있습니다. vIDM(동적) 및 Unified Access Gateway(고정) 인증자를 구성하고 활성 상태로 유지할 수 있습니다. 이러한 인증자 중 어떤 것으로도 연결할 수 있습니다.

두 개 이상의 SAML 인증자를 연결 서버에 구성하고 모든 인증자를 동시에 활성 상태로 전환할 수 있습니다. 그러나 연결 서버에 구성된 이러한 SAML 인증자 각각의 엔티티 ID는 서로 달라야 합니다.

대시보드에서 SAML 인증자는 미리 정의되어 기본적으로 고정된 메타데이터이므로 항상 상태가 녹색입니다. 빨간색과 녹색의 전환은 동적 인증자에서만 가능합니다.

VMware Unified Access Gateway 장치의 SAML 인증자 구성에 대한 자세한 내용은 Unified Access Gateway 배포 및 구성의 내용을 참조하십시오.

사전 요구 사항

- Workspace ONE, VMware Identity Manager 또는 타사 게이트웨이나 로드 밸런서가 설치 및 구성되어 있는지 확인합니다. 해당 제품의 설치 설명서를 참조하십시오.
- SAML 서버 인증서의 서명 CA에 대한 루트 인증서가 연결 서버 호스트에 설치되어 있는지 확인합니다. 자체 서명된 인증서를 사용하도록 SAML 인증자를 구성하지 않는 것이 좋습니다. 인증서 인증에 대한 자세한 내용은 Horizon 7 설치 문서를 참조하십시오.
- Workspace ONE 서버, VMware Identity Manager 서버 또는 외부 연결 로드 밸런서의 FQDN이나 IP 주소를 기록해 둡니다.
- (선택 사항) Workspace ONE 또는 VMware Identity Manager를 사용하는 경우에는 커넥터 웹 인터페이스의 URL을 적어 둡니다.
- SAML 메타데이터를 생성하고 고정 인증자를 생성해야 하는 Unified Access Gateway나 타사 장치에 대해 인증자를 만드는 경우에는 디바이스의 절차에 따라 SAML 메타데이터를 생성한 다음 메타데이터를 복사합니다.

절차

- 1 Horizon Administrator에서 **구성 > 서버**를 선택합니다.
- 2 **연결 서버** 탭에서 SAML 인증자에 연결할 서버 인스턴스를 선택하고 **편집**을 클릭합니다.

- 3 인증 탭의 **VMware Horizon(SAML 2.0 인증자)에 인증 위임** 드롭다운 메뉴에서 해당 설정을 선택하여 SAML 인증자를 사용하거나 사용하지 않도록 설정합니다.

옵션	설명
사용 안 함	SAML 인증이 사용되지 않도록 설정됩니다. Horizon Client에서만 원격 데스크톱과 애플리케이션을 시작할 수 있습니다.
허용됨	SAML 인증을 사용하도록 설정됩니다. Horizon Client와 VMware Identity Manager 또는 타사 디바이스 모두에서 원격 데스크톱 및 애플리케이션을 실행할 수 있습니다.
필수	SAML 인증을 사용하도록 설정됩니다. VMware Identity Manager 또는 타사 디바이스에서 원격 데스크톱 및 애플리케이션을 실행할 수 있습니다. 수동으로 Horizon Client에서 데스크톱이나 애플리케이션을 시작할 수 없습니다.

각자의 요구 사항에 따라 다른 SAML 인증 설정을 가지도록 배포 내의 각 연결 서버 인스턴스를 구성할 수 있습니다.

- 4 **SAML 인증자 관리**를 클릭하고 **추가**를 클릭합니다.
- 5 SAML 2.0 인증자 추가 대화 상자에서 SAML 인증자를 구성합니다.

옵션	설명
유형	Unified Access Gateway나 타사 디바이스의 경우는 고정 을 선택합니다. VMware Identity Manager의 경우는 동적 을 선택합니다. 동적 인증자의 경우는 메타데이터 URL과 관리 URL을 지정할 수 있습니다. 고정 인증자의 경우는 먼저 Unified Access Gateway 또는 타사 디바이스에서 메타데이터를 생성하고 메타데이터를 복사한 다음 SAML 메타데이터 텍스트 상자에 붙여 넣어야 합니다.
레이블	SAML 인증자를 식별하는 고유 이름입니다.
설명	SAML 인증자에 대한 간단한 설명입니다. 이 값은 선택 사항입니다.
메타데이터 URL	(동적 인증자의 경우) SAML ID 제공자와 연결 서버 인스턴스 간에 SAML 정보를 교환하는 데 필요한 모든 정보를 검색하는 URL입니다. URL <code>https://<YOUR HORIZON SERVER NAME>/SAAS/API/1.0/GET/metadata/idp.xml</code> 에서 <YOUR HORIZON SERVER NAME> 을 클릭하고 VMware Identity Manager 서버 또는 외부 연결 로드 밸런서(타사 디바이스)의 FQDN이나 IP 주소로 바꿉니다.
관리 URL	(동적 인증자의 경우) SAML ID 공급자의 관리 콘솔에 액세스하기 위한 URL입니다. VMware Identity Manager의 경우, 이 URL은 VMware Identity Manager Connector 웹 인터페이스를 가리켜야 합니다. 이 값은 선택 사항입니다.
SAML 메타데이터	(고정 인증자의 경우) Unified Access Gateway 또는 타사 디바이스에서 생성하거나 복사한 메타데이터 텍스트입니다.
연결 서버에 대해 사용	인증자를 사용하도록 설정하려면 이 확인란을 선택합니다. 여러 인증자를 사용하도록 설정할 수 있습니다. 사용하도록 설정된 인증자만 목록에 표시됩니다.

- 6 **확인**을 클릭하여 SAML 인증자 구성을 저장합니다.

올바른 정보를 제공한 경우 자체 서명된 인증서를 수락하거나(권장하지 않음) Horizon 7 및 VMware Identity Manager 또는 타사 디바이스의 신뢰할 수 있는 인증서를 사용해야 합니다. SAML 인증자 관리 대화 상자에 새로 생성된 인증자가 표시됩니다.

- 7 Horizon Administrator 대시보드의 시스템 상태 섹션에서 **기타 구성 요소 > SAML 2.0 인증자**를 선택하고 추가한 SAML 인증자를 선택한 다음 세부 정보를 확인합니다.

구성에 성공한 경우 인증자의 상태는 녹색입니다. 인증서를 신뢰할 수 없는 경우, VMware Identity Manager를 사용할 수 없는 경우 또는 메타데이터 URL이 잘못된 경우 인증자의 상태가 빨간색으로 표시될 수 있습니다. 인증서를 신뢰할 수 없는 경우 **확인**을 클릭하여 인증서를 검증 및 수락할 수 있습니다.

다음에 수행할 작업

원격 세션이 24시간 후에 종료되지 않도록 연결 서버 메타데이터의 만료 기간을 연장합니다. [연결 서버에서 서비스 제공자 메타데이터의 만료 기간 변경](#)를 참조하십시오.

VMware Identity Manager 에 대한 프록시 지원 구성

Horizon 7에서는 VMware Identity Manager(vIDM) 서버에 대한 프록시 지원을 제공합니다. 호스트 이름 및 포트 번호와 같은 프록시 세부 정보는 ADAM 데이터베이스에서 구성할 수 있으며 HTTP 요청은 해당 프록시를 통해 라우팅됩니다.

이 기능은 온 프레미스 Horizon 7 배포가 클라우드에 호스팅된 vIDM 서버와 통신할 수 있는 하이브리드 배포를 지원합니다.

사전 요구 사항

절차

- 1 연결 서버 호스트에서 ADSI 편집 유틸리티를 시작하십시오.
- 2 다음 개체 경로에서 ADAM ADSI 트리를 확장합니다.
cd=vdi,dc=vmware,dc=int,ou=Properties,ou=Global,cn=Common Attributes.
- 3 **조치 > 속성**을 선택하고 항목 **pae-SAMLProxyName** 및 **pae-SAMLProxyPort**의 값을 추가합니다.

연결 서버에서 서비스 제공자 메타데이터의 만료 기간 변경

만료 기간을 변경하지 않으면 24시간 후에 연결 서버에서 Unified Access Gateway 장치 또는 타사 ID 제공자와 같은 SAML 인증자의 SAML 어설션 승인을 중지하며, 메타데이터 교환을 반복해야 합니다.

이 절차를 사용하여 연결 서버에서 ID 제공자로부터 SAML 어설션의 수락을 중지하기 전에 경과할 수 있는 기간(일)을 지정합니다. 이 수는 현재 만료 기간이 끝날 때 사용됩니다. 예를 들어, 현재 만료 기간이 1일인 경우 90일을 지정하면 1일이 지난 후에 연결 서버에서 만료 기간이 90일인 메타데이터를 생성합니다.

사전 요구 사항

사용하고 있는 Windows 운영 체제 버전에서 ADSI 편집 유틸리티를 사용하는 방법은 Microsoft TechNet 웹 사이트를 참조하십시오.

절차

- 1 연결 서버 호스트에서 ADSI 편집 유틸리티를 시작하십시오.

- 2 콘솔 트리에서 **연결**을 선택합니다.
- 3 **고유 이름 또는 명명 컨텍스트를 선택하거나 입력합니다** 텍스트 상자에 고유 이름 DC=vdi, DC=vmware, DC=int를 입력합니다.
- 4 컴퓨터 창에서 **localhost:389**를 선택하거나 연결 서버 호스트의 FQDN(정규화된 도메인 이름)과 포트 389를 차례로 입력합니다.
예: localhost:389 또는 mycomputer.example.com:389
- 5 ADSI 편집 트리를 확장하고 **OU=Properties**를 확장한 다음 **OU=Global**을 선택하고 오른쪽 창에서 **CN=Common**을 두 번 클릭합니다.
- 6 속성 대화상자에서 **pae-NameValuePair** 특성을 편집하여 다음 값을 추가합니다.

```
cs-samlencryptionkeyvaliditydays=number-of-days
cs-samlsigningkeyvaliditydays=number-of-days
```

이 예에서 number-of-days는 원격 연결 서버에서 SAML 어설션의 승인을 중지할 때까지 경과할 수 있는 기간(일)입니다. 이 기간이 지나면 SAML 메타데이터 교환 프로세스를 반복해야 합니다.

연결 서버를 서비스 제공자로 사용할 수 있도록 SAML 메타데이터 생성

사용할 ID 제공자에 대해 SAML 인증자를 만들고 사용하도록 설정한 후에 연결 서버 메타데이터를 생성해야 할 수 있습니다. 이 메타데이터를 사용하여 Unified Access Gateway 장치에 서비스 제공자를 생성하거나, ID 공급자인 타사 로드 밸런서를 생성할 수 있습니다.

사전 요구 사항

타사 ID 공급자 Unified Access Gateway나 타사 로드 밸런서 또는 게이트웨이에 대해 SAML 인증자를 만들었는지 확인합니다. Horizon Administrator 대시보드의 시스템 상태 섹션에서 **기타 구성 요소 > SAML 2.0 인증자**를 선택하고 추가한 SAML 인증자를 선택한 다음 세부 정보를 확인할 수 있습니다.

절차

- 1 새 브라우저 탭을 열고 URL을 입력하여 연결 서버 SAML 메타데이터를 가져옵니다.

```
https://connection-server.example.com/SAML/metadata/sp.xml
```

이 예에서 connection-server.example.com은 연결 서버 호스트의 정규화된 도메인 이름입니다.

이 페이지에는 연결 서버의 SAML 메타데이터가 표시됩니다.

- 2 **다른 이름으로 저장** 명령을 사용하여 웹 페이지를 XML 파일로 저장합니다.

예를 들어, 페이지를 이름이 connection-server-metadata.xml인 파일에 저장할 수 있습니다. 이 파일의 내용은 다음 텍스트로 시작합니다.

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```


다음에 수행할 작업

ID 제공자에 적절한 절차를 사용하여 연결 서버 SAML 메타데이터를 복사합니다.
Unified Access Gateway 또는 타사 로드 밸런서나 게이트웨이의 설명서를 참조하십시오.

여러 동적 SAML 인증자에 대한 응답 시간 고려 사항

연결 서버 인스턴스에서 SAML 2.0 인증을 선택 또는 필수로 구성하고 여러 개의 동적 SAML 인증자를 연결 서버 인스턴스와 연결할 경우, 동적 SAML 인증자 중 하나라도 연결할 수 없게 되면 다른 동적 SAML 인증자에서 원격 데스크톱을 실행하는 응답 시간이 길어집니다.

Horizon Administrator를 사용하여 연결할 수 없는 동적 SAML 인증자를 사용하지 않도록 설정하면 다른 동적 SAML 인증자에서 원격 데스크톱의 실행을 위한 응답 시간을 줄일 수 있습니다. SAML 인증자를 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 [Horizon Administrator에서 SAML 인증자 구성](#)을 참조하십시오.

Horizon Administrator에서 Workspace ONE 액세스 정책 구성

Workspace ONE 또는 VMware Identity Manager(vIDM) 관리자는 Horizon 7에서 사용 권한이 있는 데스크톱 및 애플리케이션으로 액세스를 제한하도록 액세스 정책을 구성할 수 있습니다.

vIDM에서 생성된 정책을 적용하려면 Horizon 클라이언트가 사용자 정보를 Workspace ONE 클라이언트에 푸시하여 권한을 실행할 수 있도록 Horizon Client를 Workspace ONE 모드로 전환합니다. Horizon Client에 로그인할 경우 액세스 정책은 사용자가 Workspace ONE을 통해 로그인하여 게시된 데스크톱 및 애플리케이션에 액세스할 수 있도록 합니다.

사전 요구 사항

- Workspace ONE에서 애플리케이션에 대한 액세스 정책을 구성합니다. 액세스 정책 설정에 대한 자세한 내용은 VMware Identity Manager 관리 가이드를 참조하십시오.
- Horizon Administrator에서 게시된 데스크톱 및 애플리케이션에 대한 권한을 사용자에게 부여합니다.

절차

- 1 Horizon Administrator에서 **구성 > 서버**를 선택합니다.
- 2 **연결 서버** 탭에서 SAML 인증자에 연결되는 서버 인스턴스를 선택하고 **편집**을 클릭합니다.
- 3 **인증** 탭에서 **VMware Horizon(SAML 2.0 인증자)에 인증 위임** 옵션을 **필수**로 설정합니다.
[필수] 옵션을 지정하면 SAML 인증이 사용되도록 설정됩니다. 최종 사용자는 vIDM 또는 타사 ID 제공자가 제공하는 SAML 토큰으로 Horizon Server에만 연결할 수 있습니다. 수동으로 Horizon Client에서 데스크톱이나 애플리케이션을 실행할 수 없습니다.
- 4 **Workspace ONE 모드 사용**을 선택합니다.
- 5 **Workspace ONE 서버 호스트 이름** 텍스트 상자에 Workspace ONE 호스트 이름 FQDN 값을 입력합니다.

- 6 (선택 사항) **Workspace ONE** 모드를 지원하지 않는 클라이언트의 연결 차단을 선택하여 Workspace ONE 모드를 지원하는 Horizon Client가 애플리케이션에 액세스하지 못하게 제한합니다.

4.5 이전 버전의 Horizon Client는 Workspace ONE 모드 기능을 지원하지 않습니다. 이 옵션을 선택하면 4.5 이전의 Horizon Client는 Workspace ONE에서 애플리케이션에 액세스할 수 없습니다. Workspace ONE 모드 기능은 Workspace ONE 버전이 버전 2.9.1보다 이전 버전이면 Horizon 7 버전 7.2 이후 버전에서 사용되지 않도록 설정됩니다.

생체 인식 인증 구성

LDAP 데이터베이스에서 pae-ClientConfig 특성을 편집하여 생체 인식 인증을 구성할 수 있습니다.

사전 요구 사항

사용하고 있는 Windows Server에서 ADSI 편집 유틸리티를 사용하는 방법은 Microsoft TechNet 웹 사이트를 참조하십시오.

절차

- 1 연결 서버 호스트에서 ADSI 편집 유틸리티를 시작합니다.
- 2 연결 설정 대화 상자에서 **DC=vdi,DC=vmware,DC=int**를 선택하거나 연결합니다.
- 3 컴퓨터 창에서 **localhost:389**를 선택하거나 연결 서버 호스트의 FQDN(정규화된 도메인 이름)과 포트 389를 차례로 입력합니다.

예: localhost:389 또는 mycomputer.mydomain.com:389

- 4 **CN=Common, OU=Global, OU=Properties** 개체에서 **pae-ClientConfig** 특성을 편집하고 **BioMetricsTimeout=<integer>** 값을 추가합니다.

다음 BioMetricsTimeout 값이 유효합니다.

BioMetricsTimeout 값	설명
0	생체 인식 인증이 지원되지 않습니다. 이것이 기본값입니다.
-1	생체 인식 인증은 시간 제한 없이 지원됩니다.
모든 양의 정수	생체 인식 인증이 지원되며 지정된 시간(분) 동안 사용할 수 있습니다.

새로운 설정은 즉시 적용됩니다. 연결 서버 서비스 또는 클라이언트 디바이스를 다시 시작할 필요가 없습니다.

자격 증명을 요구하지 않고 사용자 인증

5

사용자는 클라이언트 디바이스나 VMware Identity Manager에 로그인한 후에 Active Directory 자격 증명을 요구하는 프롬프트 없이 게시된 애플리케이션이나 데스크톱에 연결할 수 있습니다.

관리자는 사용자 요구 사항에 따라 구성을 설정하도록 선택할 수 있습니다.

- 사용자에게 게시된 애플리케이션에 대해 인증되지 않은 액세스를 제공합니다. 관리자는 사용자가 Horizon Client에 로그인할 때 AD(Active Directory) 자격 증명을 사용할 필요가 없도록 설정을 구성할 수 있습니다.
- Windows 기반 클라이언트에 대해 [현재 사용자로 로그인]을 사용합니다. Windows 기반 클라이언트의 경우 관리자는 사용자가 AD 자격 증명으로 Windows 기반 클라이언트에 로그인한 후에 Horizon Server에 로그인할 때 추가 자격 증명을 제공할 필요가 없도록 설정을 구성할 수 있습니다.
- 모바일 및 Mac 클라이언트에서 자격 증명을 저장합니다. 모바일 및 Mac 클라이언트의 경우 관리자는 Horizon Server에서 자격 증명을 저장하도록 구성할 수 있습니다. 이 기능으로 모바일 또는 Mac 클라이언트에 SSO(Single Sign-On)용 AD 자격 증명을 한 번 제공하게 되면 사용자는 더 이상 해당 자격 증명을 기억할 필요가 없습니다.
- VMware Identity Manager에 대해 True SSO를 구성합니다. VMware Identity Manager의 경우 관리자는 AD 자격 증명이 아닌 방법으로 인증한 사용자가 AD 자격 증명을 요구하는 프롬프트 없이 게시된 데스크톱이나 애플리케이션에도 로그인할 수 있도록 True SSO를 구성할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 게시된 애플리케이션에 대해 인증되지 않은 액세스 제공
- 하이브리드 로그인에 대해 사용자 구성
- Windows 기반 Horizon Client에서 제공하는 현재 사용자로 로그인 기능 사용
- 모바일 및 Mac Horizon Client에서 자격 증명 저장
- True SSO 설정

게시된 애플리케이션에 대해 인증되지 않은 액세스 제공

관리자는 AD 자격 증명을 요구하지 않으면서 인증되지 않은 사용자가 Horizon Client에서 게시된 애플리케이션에 액세스할 수 있도록 구성을 설정할 수 있습니다. 사용자가 자체 보안 및 사용자 관리가 적용되는 원활한 애플리케이션에 액세스해야 할 경우 인증되지 않은 액세스를 설정하는 것을 고려하십시오.

사용자가 인증되지 않은 액세스용으로 구성된 게시된 애플리케이션을 시작할 경우 RDS 호스트는 필요할 때 로컬 사용자 세션을 생성하고 해당 세션을 사용자에게 할당합니다.

이 기능에는 Horizon Client 버전 4.4 이상이 필요합니다. HTML Access 클라이언트의 경우 이 기능을 사용하려면 버전 4.5 이상이 필요합니다.

인증되지 않은 사용자 구성 워크플로

- 1 인증되지 않은 액세스의 사용자를 생성합니다. [인증되지 않은 액세스의 사용자 생성](#)을 참조하십시오.
- 2 사용자에게 인증되지 않은 액세스를 사용하도록 설정하고 인증되지 않은 기본 사용자를 설정합니다. [사용자의 인증되지 않은 액세스 사용](#)을 참조하십시오.
- 3 인증되지 않은 사용자에게 게시된 애플리케이션에 대한 사용 권한을 부여합니다. [인증되지 않은 액세스 사용자에게 게시된 애플리케이션에 대한 사용 권한 부여](#)을 참조하십시오.
- 4 Horizon Client에서의 인증되지 않은 액세스를 사용하도록 설정합니다. [Horizon Client의 인증되지 않은 액세스](#)를 참조하십시오.

인증되지 않은 사용자 구성 규칙 및 지침

- RSA 및 RADIUS와 같은 2단계 인증과 스마트 카드 인증은 인증되지 않은 액세스에 대해 지원되지 않습니다.
- 스마트 카드 인증 및 인증되지 않은 액세스는 상호 배타적입니다. 연결 서버에서 스마트 카드 인증이 필수로 설정되면 이전에 사용되도록 설정되었어도 인증되지 않은 액세스는 사용되도록 설정되지 않습니다.
- VMware Identity Manager 및 VMware App Volumes는 인증되지 않은 액세스에 대해 지원되지 않습니다.
- PCoIP 및 VMware Blast 디스플레이 프로토콜 둘 다 이 기능에 대해 지원됩니다.
- 인증되지 않은 액세스 기능은 RDS 호스트에 대한 라이선스 정보를 확인하지 않습니다. 관리자는 디바이스 라이선스를 구성하고 사용해야 합니다.
- 인증되지 않은 액세스 기능은 사용자별 데이터를 보존하지 않습니다. 사용자는 애플리케이션에 대한 데이터 스토리지 요구 사항을 확인할 수 있습니다.
- 인증되지 않은 애플리케이션 세션에 다시 연결할 수 없습니다. 사용자가 클라이언트에서 연결 해제되면 RDS 호스트는 로컬 사용자 세션에서 자동으로 로그오프됩니다.
- 인증되지 않은 액세스는 게시된 애플리케이션에 대해서만 지원됩니다.

- 인증되지 않은 액세스는 보안 서버 또는 Unified Access Gateway 장치에서 지원되지 않습니다.
- 인증되지 않은 사용자의 사용자 기본 설정은 보존되지 않습니다.
- 가상 데스크톱은 인증되지 않은 사용자에게 지원되지 않습니다.
- Horizon Administrator는 연결 서버가 CA 서명 인증서로 구성되어 있고 인증되지 않은 액세스에 대해 사용되도록 설정되어 있으나 인증되지 않은 기본 사용자가 구성되지 않은 경우 연결 서버에 대해 빨간색 상태를 표시합니다.
- RDS 호스트에 설치된 Horizon Agent에 대해 AllowSingleSignon 그룹 정책 설정이 사용되지 않도록 설정되어 있으면 인증되지 않은 액세스 기능은 작동하지 않습니다. 또한 관리자는 UnAuthenticatedAccessEnabled Horizon Agent 그룹 정책 설정을 사용하여 인증되지 않은 액세스를 사용하지 않도록 설정할지 또는 사용하도록 설정할지를 제어할 수 있습니다. Horizon Agent 그룹 정책 설정은 vdm_agent.admx 템플릿 파일에 포함되어 있습니다. 이 정책이 적용되려면 RDS 호스트를 재부팅해야 합니다.

인증되지 않은 액세스의 사용자 생성

관리자는 게시된 애플리케이션에 대해 인증되지 않은 액세스의 사용자를 생성할 수 있습니다. 관리자가 인증되지 않은 액세스의 사용자를 구성하면 해당 사용자는 인증되지 않은 액세스만으로 Horizon Client에서 연결 서버 인스턴스에 로그인할 수 있습니다.

사전 요구 사항

- 인증되지 않은 액세스를 구성하려는 AD(Active Directory) 사용자에게 유효한 UPN이 있는지 확인합니다. AD 사용자만 인증되지 않은 액세스 사용자로 구성할 수 있습니다.

참고 관리자는 각 AD 계정에 대해 하나의 사용자만 생성할 수 있습니다. 관리자는 인증되지 않은 사용자 그룹을 생성할 수 없습니다. 인증되지 않은 액세스 사용자를 생성할 때 해당 AD 사용자에게 대한 기존 클라이언트 세션이 있는 경우 변경 내용을 적용하려면 클라이언트 세션을 다시 시작해야 합니다.

절차

- 1 Horizon Administrator에서 **사용자 및 그룹**을 선택합니다.
- 2 **인증되지 않은 액세스** 탭에서 **추가**를 클릭합니다.
- 3 **인증되지 않은 사용자 추가** 마법사에서 하나 이상의 검색 조건을 선택하고 **찾기**를 클릭하여 검색 조건에 따라 사용자를 찾습니다.
사용자에게 유효한 UPN이 있어야 합니다.
- 4 사용자를 선택하고 **다음**을 클릭합니다.
여러 사용자를 추가하려면 이 단계를 반복하십시오.
- 5 (선택 사항) 사용자 별칭을 입력합니다.
기본 사용자 별칭은 AD 계정에 대해 구성된 사용자 이름입니다. 최종 사용자는 사용자 별칭을 사용하여 Horizon Client에서 연결 서버 인스턴스에 로그인할 수 있습니다.

6 (선택 사항) 사용자 세부 정보를 검토하고 설명을 추가합니다.

7 **마침**을 클릭합니다.

연결 서버는 인증되지 않은 액세스 사용자를 생성하고 사용자 별칭, 사용자 이름, 성과 이름, 소스 포트 수, 애플리케이션 사용 권한 및 세션을 비롯한 사용자 세부 정보를 표시합니다. [소스 포트] 열의 숫자를 클릭하여 포트 정보를 표시할 수 있습니다.

다음에 수행할 작업

연결 서버의 사용자에게 인증되지 않은 액세스를 사용하도록 설정합니다. [사용자의 인증되지 않은 액세스 사용](#)을 참조하십시오.

사용자의 인증되지 않은 액세스 사용

인증되지 않은 액세스의 사용자를 생성한 후에는 연결 서버에서 인증되지 않은 액세스를 사용하도록 설정하여 사용자가 게시된 애플리케이션에 연결하고 액세스할 수 있도록 해야 합니다.

절차

1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.

2 **연결 서버** 탭을 클릭합니다.

3 연결 서버 인스턴스를 선택하고 **편집**을 클릭합니다.

4 **인증** 탭을 클릭합니다.

5 **인증되지 않은 액세스**를 **활성화**로 변경합니다.

6 **인증되지 않은 기본 액세스 사용자** 드롭다운 메뉴에서 사용자를 기본 사용자로 선택합니다.

기본 사용자는 Cloud Pod 아키텍처 환경의 로컬 포트에 있어야 합니다. 다른 포트에서 기본 사용자를 선택하는 경우 연결 서버는 사용자를 기본 사용자로 설정하기 전에 로컬 포트에서 해당 사용자를 생성합니다.

7 (선택 사항) 사용자에게 대한 기본 세션 시간 초과를 입력합니다.

기본 세션 시간 초과는 유효 상태가 되고 10분 후입니다.

8 **확인**을 클릭합니다.

다음에 수행할 작업

인증되지 않은 사용자에게 게시된 애플리케이션에 대한 사용 권한을 부여합니다. [인증되지 않은 액세스 사용자에게 게시된 애플리케이션에 대한 사용 권한 부여](#)의 내용을 참조하십시오.

인증되지 않은 액세스 사용자에게 게시된 애플리케이션에 대한 사용 권한 부여

인증되지 않은 액세스 사용자를 생성한 후에는 해당 사용자가 게시된 애플리케이션에 액세스하도록 사용 권한을 부여해야 합니다.

사전 요구 사항

- RDS 호스트 그룹을 기준으로 팜을 생성합니다. Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정 문서에서 “팜 생성”을 참조하십시오.
- RDS 호스트 팜에서 실행되는 게시된 애플리케이션에 대해 애플리케이션 풀을 생성합니다. Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정 문서에서 “애플리케이션 풀 생성”을 참조하십시오.

절차

- 1 Horizon Administrator에서 **카탈로그 > 애플리케이션 풀**을 선택하고 애플리케이션 풀 이름을 클릭합니다.
- 2 **권한** 드롭다운 메뉴에서 **권한 추가**를 선택합니다.
- 3 **추가**를 클릭하고 하나 이상의 검색 조건을 선택한 후 **찾기**를 클릭하고 **인증되지 않은 사용자** 확인란을 선택하여 검색 조건에 따라 인증되지 않은 액세스 사용자를 찾습니다.
- 4 풀의 애플리케이션에 대해 사용 권한을 부여할 사용자를 선택하고 **확인**을 클릭합니다.
- 5 변경 사항을 저장하려면 **확인**을 클릭합니다.

사용 권한 부여 프로세스가 완료되면 인증되지 않은 액세스 사용자 옆에 인증되지 않은 액세스 아이콘이 표시됩니다.

다음에 수행할 작업

인증되지 않은 액세스 사용자를 사용하여 Horizon Client에 로그인합니다. [Horizon Client의 인증되지 않은 액세스](#)를 참조하십시오.

인증되지 않은 액세스 세션 검색

Horizon Administrator를 사용하여 인증되지 않은 액세스 사용자가 연결된 애플리케이션 세션을 나열하거나 검색할 수 있습니다. 인증되지 않은 액세스 사용자가 연결된 세션 옆에 인증되지 않은 액세스 사용자 아이콘이 표시됩니다.

절차

- 1 Horizon Administrator에서 **모니터링 > 세션**을 선택합니다.
- 2 **애플리케이션**을 클릭하여 애플리케이션 세션을 검색합니다.
- 3 검색 조건을 선택하고 검색을 시작합니다.

검색 결과에는 사용자, 세션 유형(데스크톱 또는 애플리케이션), 시스템, 풀 또는 팜, DNS 이름, 클라이언트 ID 및 보안 게이트웨이가 포함됩니다. 세션 시작 시간, 지속 시간, 상태 및 마지막 세션도 검색 결과에 표시됩니다.

인증되지 않은 액세스 사용자 삭제

인증되지 않은 액세스 사용자를 삭제할 경우 해당 사용자의 애플리케이션 풀 사용 권한도 제거해야 합니다. 인증되지 않은 액세스 사용자가 기본 사용자인 경우에는 삭제할 수 없습니다.

참고 인증되지 않은 액세스 사용자를 삭제할 때 해당 AD 사용자에 대한 기존 클라이언트 세션이 있는 경우 변경 내용을 적용하려면 클라이언트 세션을 다시 시작해야 합니다.

절차

- 1 Horizon Administrator에서 **사용자 및 그룹**을 선택합니다.
- 2 **인증되지 않은 액세스** 탭에서 **삭제**를 클릭합니다.
- 3 **확인**을 클릭합니다.

다음에 수행할 작업

사용자의 애플리케이션 사용 권한을 제거합니다. Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정 문서에서 “데스크톱 또는 애플리케이션 풀에서 권한 제거”를 참조하십시오.

Horizon Client 의 인증되지 않은 액세스

인증되지 않은 액세스로 Horizon Client에 로그인하고 게시된 애플리케이션을 시작합니다.

보안을 강화하기 위해 인증되지 않은 액세스 사용자는 Horizon Client에 로그인하는 데 사용할 수 있는 사용자 별칭을 갖습니다. 사용자 별칭을 선택하는 경우 사용자에게 대한 AD 자격 증명이나 UPN을 제공할 필요가 없습니다. Horizon Client에 로그인한 후에 게시된 애플리케이션을 클릭하여 애플리케이션을 시작할 수 있습니다. Horizon Client 설치 및 설정에 대한 자세한 내용은 [VMware Horizon Client 설명서](#) 웹 페이지에서 Horizon Client 설명서를 참조하십시오.

사전 요구 사항

- Horizon 7 버전 7.1 연결 서버가 인증되지 않은 액세스에 대해 구성되어 있는지 확인합니다.
- 인증되지 않은 액세스 사용자가 Horizon Administrator에 생성되어 있는지 확인합니다. 인증되지 않은 기본 사용자가 유일한 인증되지 않은 액세스 사용자인 경우 Horizon Client에서 기본 사용자로 연결 서버 인스턴스에 연결합니다.

절차

- 1 Horizon Client를 시작합니다.
- 2 Horizon Client에서 **인증되지 않은 액세스 기능을 사용하여 익명으로 로그인**을 선택합니다.
- 3 연결 서버 인스턴스에 연결합니다.
- 4 드롭다운 메뉴에서 사용자 별칭을 선택하고 **로그인**을 클릭합니다.
기본 사용자에는 “default” 접미사가 있습니다.
- 5 게시된 애플리케이션을 두 번 클릭하여 애플리케이션을 시작합니다.

게시된 애플리케이션에 대한 인증되지 않은 액세스에 대해 로그인 감속 구성

사용자가 인증되지 않은 액세스를 사용할 경우 자격 증명을 입력하지 않으므로 RDS 호스트에서 게시된 애플리케이션의 과도한 요청이 발생할 수 있습니다. 로그인 감속을 사용하면 이 문제가 완화됩니다. 감속 수준을 조정할 수 있습니다. 또한 감속을 지원하지 않는 클라이언트를 차단할 수도 있습니다.

사전 요구 사항

- 사용자에게 인증되지 않은 액세스를 사용하도록 설정했는지 확인합니다.
- Horizon Client 버전 4.9 이상이 있는지 확인합니다. Horizon Client 버전 4.8을 사용하는 경우 사용자가 Horizon 7 버전 7.6에 대해 인증되지 않은 액세스 기능을 사용하여 익명으로 로그인할 경우 로그인이 실패하며, 로그인을 다시 시도해야 할 수 있습니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 **연결 서버** 탭을 클릭합니다.
- 3 **인증** 탭을 클릭합니다.
- 4 **로그인 감속 수준** 드롭다운 메뉴에서 인증되지 않은 액세스 로그인에 대한 감속 수준을 선택합니다.

옵션	설명
낮음	인증되지 않은 액세스 로그인에 대해 낮은 감속 수준을 설정합니다. Microsoft Internet Explorer 및 Microsoft Edge와 같은 웹 브라우저에서는 낮은 감속 수준이 권장됩니다.
중간	인증되지 않은 액세스 로그인에 대해 중간 감속 수준을 설정합니다. 기본적으로 이 수준으로 설정됩니다. Horizon Client 버전 4.8을 사용하는 경우에는 이 설정을 변경하지 마십시오.
높음	인증되지 않은 액세스 로그인에 대해 높은 감속 수준을 설정합니다. 높은 감속 수준을 설정하면 로그인 시간이 늘어나고 최종 사용자 환경에도 영향을 줄 수 있습니다.

- 5 (선택 사항) 로그인 감속을 지원하지 않는 모든 클라이언트가 인증되지 않은 액세스를 사용하여 Horizon 7에 연결하지 못하도록 하려면 **규정 위반 클라이언트 차단**을 선택합니다.

버전 4.8보다 이전 버전인 Horizon Client는 규정 위반 버전입니다.

- 6 **확인**을 클릭합니다.

다음에 수행할 작업

인증되지 않은 액세스로 Horizon Client에 로그인하고 게시된 애플리케이션을 시작합니다. [Horizon Client의 인증되지 않은 액세스](#)의 내용을 참조하십시오.

하이브리드 로그온에 대해 사용자 구성

인증되지 않은 액세스 사용자를 생성한 후에 사용자가 하이브리드 로그온을 사용하도록 설정할 수 있습니다. 하이브리드 로그온을 사용하도록 설정하면 인증되지 않은 액세스 사용자가 자격 증명을 입력하지 않아도 파일 공유 또는 네트워크 프린터와 같은 네트워크 리소스에 대해 도메인 액세스 권한을 갖게 됩니다.

참고 하이브리드 로그온 기능은 하이브리드 로그온에 대해 구성된 인증되지 않은 특정 액세스 사용자로 로그온한 모든 사용자에게 동일한 도메인 사용자를 사용합니다.

참고 사용자 프로필 탭을 사용하여 홈 디렉토리를 RDS 호스트 시스템의 네트워크 경로로 설정하면, 기본적으로 Windows의 관리 사용자 인터페이스는 홈 디렉토리 폴더에서 모든 기존 사용 권한을 제거하고 관리자 및 모든 권한이 있는 로컬 사용자에게 대한 사용 권한을 추가합니다. 관리자 계정을 사용하여 사용 권한 목록에서 로컬 사용자를 제거한 후 사용자에게 대해 설정해야 하는 사용 권한을 갖는 도메인 사용자를 추가합니다.

사전 요구 사항

- RDS 호스트에 Horizon Agent를 설치하는 경우 하이브리드 로그온 사용자 지정 옵션을 선택했는지 확인합니다. RDS 호스트의 Horizon Agent 사용자 지정 설치 옵션에 대한 자세한 내용은 Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정 문서를 참조하십시오.
- 인증되지 않은 액세스 사용자를 생성했는지 확인합니다.
- 도메인의 사용자 계정에 대해 Kerberos DES 암호화를 사용하도록 설정했는지 확인합니다. 하이브리드 로그온 기능에 대해 Kerberos DES 암호화가 지원되지 않습니다.

절차

- 1 Horizon Administrator에서 **사용자 및 그룹**을 선택합니다.
- 2 **인증되지 않은 액세스** 탭에서 **추가**를 클릭합니다.
- 3 **인증되지 않은 사용자 추가** 마법사에서 하나 이상의 검색 조건을 선택하고 **찾기**를 클릭하여 검색 조건에 따라 인증되지 않은 액세스 사용자를 찾습니다.
사용자에게 유효한 UPN이 있어야 합니다.
- 4 인증되지 않은 액세스 사용자를 선택하고 **다음**을 클릭합니다.
여러 사용자를 추가하려면 이 단계를 반복하십시오.
- 5 (선택 사항) 사용자 별칭을 입력합니다.
기본 사용자 별칭은 AD 계정에 대해 구성된 사용자 이름입니다. 최종 사용자는 사용자 별칭을 사용하여 Horizon Client에서 연결 서버 인스턴스에 로그인할 수 있습니다.
- 6 (선택 사항) 사용자 세부 정보를 검토하고 설명을 추가합니다.

7 하이브리드 로그인 사용을 선택합니다.

True SSO 사용 옵션은 기본적으로 선택되어 있습니다. Horizon 7 환경에 대해 True SSO를 사용하도록 설정해야 합니다. 그러면 하이브리드 로그인을 사용하도록 설정된 인증되지 않은 액세스 사용자는 True SSO를 사용하여 Horizon Client에서 연결 서버 인스턴스에 로그인합니다.

참고 연결 서버 포트가 True SSO에 대해 구성되지 않은 경우 사용자는 인증되지 않은 액세스 권한으로 권한 있는 애플리케이션을 시작할 수 있습니다. 그러나 포트에서 True SSO를 사용하도록 설정되지 않으므로 사용자에게 네트워크 액세스 권한이 없습니다.

8 (선택 사항) 사용자가 Horizon Client에서 연결 서버 인스턴스에 로그인할 수 있도록 하려면 **암호 로그인 사용**을 선택하고 사용자의 암호를 입력합니다.

Horizon 7 환경에 대해 True SSO가 구성되지 않은 경우 이 설정을 사용합니다.

CPA 환경에서 하이브리드 로그인 사용자 기능은 하이브리드 로그인 사용자가 **암호 로그인 사용** 설정으로 구성되었으며 게시된 애플리케이션에 대해 사용 권한이 있는 연결 서버 포트에서만 작동합니다.

예를 들어 포트 A와 포트 B가 있는 CPA 환경에서 **암호 로그인 사용** 설정으로 구성된 하이브리드 로그인 사용자는 포트 A의 애플리케이션에 대한 사용 권한이 부여됩니다. 이 사용자는 포트 A 또는 포트 B에 연결된 클라이언트에서 애플리케이션을 보고 시작할 수 있습니다. 그러나 포트 B의 동일한 사용자에게 다른 애플리케이션에 대한 사용 권한이 부여되면 해당 사용자는 포트 B에 연결된 클라이언트에서 애플리케이션을 보고 시작할 수 없습니다. 포트 B에서 하이브리드 로그인 기능을 사용하려면 **암호 로그인 사용** 설정으로 구성된 또 다른 하이브리드 로그인 사용자를 생성하고 해당 사용자에게 애플리케이션에 대한 사용 권한을 부여해야 합니다. CPA 환경 설정 방법에 대한 자세한 내용은 Horizon 7에서 Cloud Pod 아키텍처 관리 문서를 참조하십시오.

9 마침을 클릭합니다.

다음에 수행할 작업

게시된 애플리케이션에 대한 사용 권한을 사용자에게 부여합니다. [인증되지 않은 액세스 사용자에게 게시된 애플리케이션에 대한 사용 권한 부여](#)의 내용을 참조하십시오.

Windows 기반 Horizon Client 에서 제공하는 현재 사용자 로 로그인 기능 사용

Windows용 Horizon Client에서는 사용자가 **옵션** 메뉴에서 **현재 사용자로 로그인**을 선택하면 클라이언트 시스템에 로그인할 때 입력했던 자격 증명을 사용해 Horizon 연결 서버 인스턴스와 원격 데스크톱에 대해 사용자를 인증합니다. 추가 사용자 인증은 필요하지 않습니다.

이 기능을 사용하려면 연결 서버 인스턴스와 클라이언트 시스템에 사용자 자격 증명에 저장되어 있어야 합니다.

- 연결 서버 인스턴스에서는 사용자 이름, 도메인, 선택적 UPN과 함께 사용자 자격 증명에 암호화되어 사용자 세션에 저장됩니다. 자격 증명은 인증 작업 수행 시 추가되고 세션 개체 삭제 시 제거됩니다. 사용자가 로그아웃하거나 세션 시간이 초과하거나 인증이 실패하면 세션 개체가 지워집니다. 세션 개체는 휘발성 메모리에 상주하며 Horizon LDAP 또는 디스크 파일에 저장되지 않습니다.

- 연결 서버 인스턴스에서 **현재 사용자로 로그인** 수락 설정을 사용하도록 설정하여 사용자가 Horizon Client의 **옵션** 메뉴에서 **현재 사용자로 로그인**을 선택할 때 제공된 사용자 ID 및 자격 증명 정보를 연결 서버 인스턴스가 수락하도록 합니다.

중요 이 설정을 사용하도록 설정하기 전에 보안 위험을 파악해야 합니다. Horizon 7 보안 문서에서 "사용자 인증에 대한 보안 관련 서버 설정"을 참조하십시오.

- 클라이언트 시스템에서는 사용자 자격 증명이 암호화되어 Horizon Client의 구성 요소인 인증 패키지에 있는 테이블에 저장됩니다. 자격 증명은 사용자가 로그인하면 테이블에 추가되고 사용자가 로그아웃하면 테이블에서 제거됩니다. 테이블은 휘발성 메모리에 상주합니다.

관리자는 Horizon Client 그룹 정책 설정을 사용하여 **옵션** 메뉴에 있는 **현재 사용자로 로그인** 설정의 사용 가능 여부를 제어하고 기본값을 지정합니다. 관리자는 또한 그룹 정책을 통해 사용자가 Horizon Client에서 **현재 사용자로 로그인**을 선택할 때 전달되는 사용자 ID 및 자격 증명 정보를 수락할 연결 서버 인스턴스를 지정합니다.

재귀 잠금 해제 기능은 사용자가 현재 사용자로 로그인 기능을 사용해서 연결 서버에 로그인한 후에 사용되도록 설정됩니다. 재귀 잠금 해제 기능은 클라이언트 시스템이 잠금 해제된 후에 모든 원격 세션의 잠금을 해제합니다. 관리자는 Horizon Client의 **클라이언트 시스템이 잠금 해제될 때 원격 세션 잠금 해제** 글로벌 정책 설정으로 재귀 잠금 해제 기능을 제어할 수 있습니다. Horizon Client에 대한 글로벌 정책 설정에 대한 자세한 내용은 [VMware Horizon Clients 설명서](#) 웹 페이지에서 Horizon Client 설명서를 참조하십시오.

현재 사용자로 로그인 기능은 다음과 같은 제한 사항이 있습니다.

- 연결 서버 인스턴스에 대해 스마트 카드 인증이 [필수]로 설정되어 있는 경우 사용자가 **현재 사용자로 로그인**을 선택하고 연결 서버 인스턴스에 연결하면 인증에 실패합니다. 이들 사용자는 연결 서버에 로그인할 때 스마트 카드와 PIN으로 재인증해야 합니다.
- 클라이언트가 로그인하는 시스템 시간과 연결 서버 호스트 시간이 동기화되어 있어야 합니다.
- 클라이언트 시스템에서 기본 **네트워크에서 이 컴퓨터 액세스** 사용자 권한 할당을 수정한 경우 VMware 기술 자료(KB) 문서 1025691에 따라 수정해야 합니다.
- 클라이언트 시스템은 기업 Active Directory 서버와 통신할 수 있어야 하며 캐시된 자격 증명을 인증에 사용하면 안 됩니다. 예를 들어 사용자가 기업 네트워크 외부에서 클라이언트 시스템으로 로그인할 경우, 캐시된 자격 증명이 인증에 사용됩니다. 사용자가 VPN 연결을 먼저 설정하지 않고 보안 서버 또는 연결 서버 인스턴스에 연결할 경우, 사용자에게 자격 증명을 묻는 메시지가 나타나며 현재 사용자로 로그인 기능이 작동하지 않습니다.

모바일 및 Mac Horizon Client에서 자격 증명 저장

관리자는 모바일 및 Mac Horizon Client에서 사용자의 사용자 이름, 암호 및 도메인 정보를 기억하도록 연결 서버를 구성할 수 있습니다.

모바일 디바이스용 Horizon Client에서 이 기능을 사용하면 로그인 대화상자에 **암호 저장** 확인란이 나타납니다. Mac용 Horizon Client에서 이 기능을 사용하면 로그인 대화상자에 **이 암호 기억** 확인란이 나타납니다.

사용자가 자신의 자격 증명을 저장하도록 선택하면 후속 연결 시 자격 증명에 Horizon Client의 로그인 필드에 추가됩니다.

이 기능을 사용하도록 설정하려면 View LDAP의 값을 설정하여 클라이언트에서 자격 증명 정보를 저장할 기간을 나타내야 합니다. Mac용 Horizon Client의 경우 이 기능은 버전 4.1 이상에서만 지원됩니다.

참고 Windows 기반 Horizon 클라이언트에서 현재 사용자로 로그인하는 기능을 사용하면 사용자가 자격 증명을 여러 번 제공하지 않아도 됩니다.

Horizon Client 자격 증명을 저장하기 위한 시간 제한 구성

View LDAP에서 값을 설정하여 모바일 디바이스 및 Mac 클라이언트 시스템에 Horizon Client 자격 증명 정보를 저장할 기간을 나타내는 시간 초과 제한을 구성합니다. 시간 초과 제한이 분 단위로 설정됩니다. 연결 서버 인스턴스의 View LDAP를 변경하면 모든 복제된 연결 서버 인스턴스에 변경 사항이 적용됩니다.

사전 요구 사항

사용하고 있는 Windows 운영 체제 버전에서 ADSI 편집 유틸리티를 사용하는 방법은 Microsoft TechNet 웹 사이트를 참조하십시오.

절차

- 1 연결 서버 호스트에서 ADSI 편집 유틸리티를 시작하십시오.
- 2 연결 설정 대화 상자에서 **DC=vdi,DC=vmware,DC=int**를 선택하거나 연결합니다.
- 3 컴퓨터 창에서 **localhost:389**를 선택하거나 연결 서버 호스트의 FQDN(정규화된 도메인 이름)과 포트 389를 차례로 입력합니다.

예: **localhost:389** 또는 **mycomputer.mydomain.com:389**

- 4 **CN=Common, OU=Global, OU=Properties** 개체에서 **clientCredentialCacheTimeout** 특성 값을 편집합니다.

clientCredentialCacheTimeout을 설정하지 않거나 **0**으로 설정하면 기능이 사용되지 않습니다. 이 기능을 사용하려면 자격 증명 정보를 유지할 시간(분)을 설정하거나 시간 제한이 없음을 의미하는 값인 **-1**을 설정하면 됩니다.

연결 서버에서 새 설정이 바로 적용됩니다. 연결 서버 서비스 또는 클라이언트 컴퓨터를 다시 시작할 필요가 없습니다.

True SSO 설정

True SSO(Single Sign-On) 기능을 사용하면, 스마트 카드나 RSA SecurID 또는 RADIUS 인증을 사용하여 VMware Identity Manager에 로그인한 후에 사용자가 가상 데스크톱 또는 게시된 데스크톱이나 애플리케이션을 사용하기 위해 Active Directory 자격 증명을 입력할 필요가 없습니다.

사용자가 Active Directory 자격 증명을 사용하여 인증한 경우에는 True SSO 기능이 필요하지 않지만, 이 경우에도 True SSO를 사용하도록 구성하여 사용자가 제공하는 AD 자격 증명을 무시하고 True SSO를 사용하도록 할 수 있습니다.

가상 데스크톱이나 게시된 애플리케이션에 연결할 때 사용자는 기본 Horizon Client 또는 HTML Access를 사용하도록 선택할 수 있습니다.

이 기능의 제한 사항은 다음과 같습니다.

- View Agent Direct Connection 플러그인을 사용하여 제공되는 가상 데스크톱에서는 이 기능이 작동하지 않습니다.
- 이 기능은 IPv4 환경에서만 지원됩니다.

다음은 True SSO에 대해 환경을 설정할 때 수행해야 하는 작업의 목록입니다.

- 1 [True SSO의 아키텍처 확인](#)
- 2 [Enterprise CA 설정](#)
- 3 [True SSO에 사용하는 인증서 템플릿 만들기](#)
- 4 [등록 서버 설치 및 설정](#)
- 5 [등록 서비스 클라이언트 인증서 내보내기](#)
- 6 [SAML 인증이 True SSO에서 작동하도록 구성](#)
- 7 [True SSO에 대한 Horizon 연결 서버 구성](#)

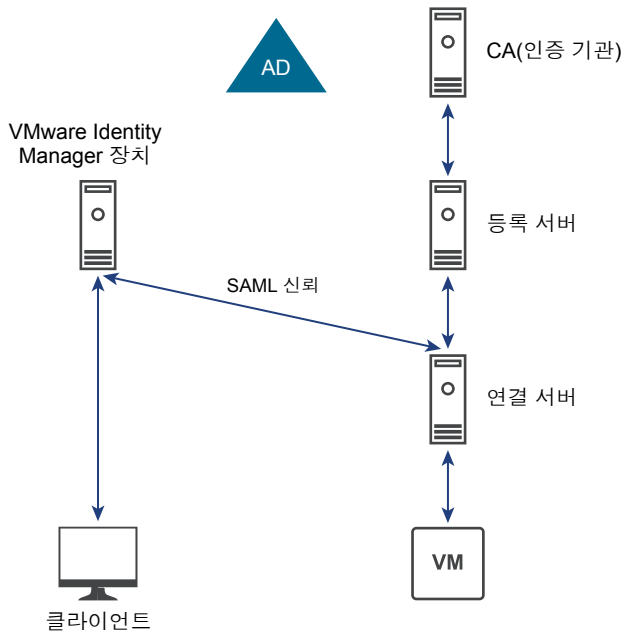
True SSO의 아키텍처 확인

True SSO를 사용하려는 경우 CA(인증 기관)가 이미 있지 않으면 추가해야 하며 등록 서버를 만들어야 합니다. 이 두 서버는 서로 통신하며 암호 없이 Windows에 로그인할 수 있는, 일시적인 Horizon 가상 인증서를 만듭니다. True SSO는 단일 도메인, 다중 도메인이 있는 단일 포리스트, 다중 포리스트, 다중 도메인 설정에서 사용할 수 있습니다.

VMware에서는 두 개의 CA와 두 개의 ES를 배포하여 True SSO에 사용할 것을 권장합니다. 다음 예에서는 서로 다른 아키텍처의 True SSO를 보여 줍니다.

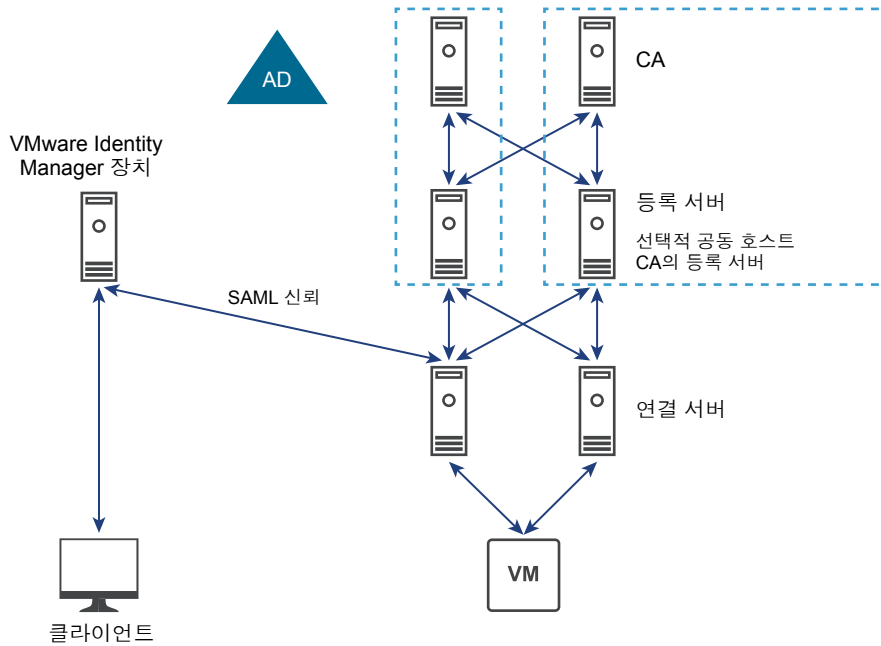
다음 그림에서는 단순한 True SSO 아키텍처를 보여 줍니다.

매우 단순한 True SSO 아키텍처



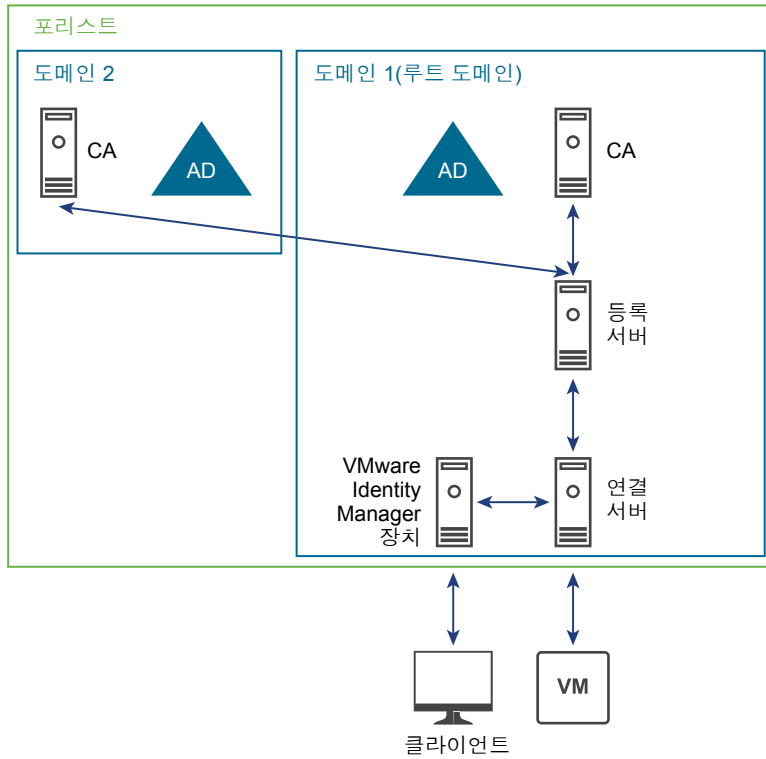
다음 그림에서는 단일 도메인 아키텍처의 True SSO를 보여 줍니다.

일반적인 HA True SSO 아키텍처(단일 도메인)



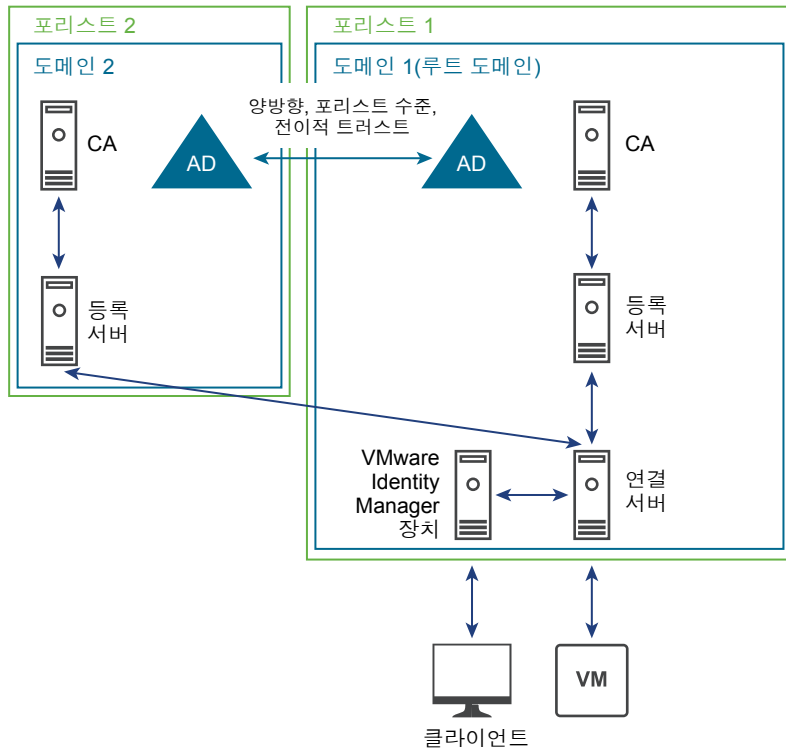
다음 그림에서는 다중 도메인 아키텍처가 있는 단일 포리스트의 True SSO를 보여 줍니다.

True SSO 단일 포리스트 다중 도메인 아키텍처(HA 아님)



다음 그림에서는 다중 포리스트 아키텍처의 True SSO를 보여 줍니다.

True SSO 다중 포리스트 아키텍처(HA 아님)



Enterprise CA 설정

이미 CA(인증 기관)가 설정되어 있지 않은 경우에는 Windows 서버에 AD CS(Active Directory Certificate Services) 역할을 추가하고 서버를 Enterprise CA로 구성해야 합니다.

Enterprise CA가 이미 설정되어 있지 않은 경우는 이 절차에 설명된 설정을 사용하고 있는지 확인합니다.

Enterprise CA가 하나 이상 있어야 하며, VMware는 페일오버와 로드 밸런싱을 위해 두 개를 사용할 것을 권장합니다. True SSO용으로 만들 등록 서버는 Enterprise CA와 통신합니다. 환경 서버에서 여러 Enterprise CA를 사용하도록 구성한 경우에는 등록 서버에서 사용 가능한 CA를 번갈아 사용합니다. Enterprise CA를 호스팅하는 동일한 시스템에 등록 서버를 설치하면 등록 서버에서 로컬 CA를 기본으로 사용하도록 구성할 수 있습니다. 이 구성은 최상의 성능을 위해 권장됩니다.

이 절차의 일부는 비영구 인증서 처리를 사용하도록 설정하는 것과 관련되어 있습니다. 기본적으로 인증서 처리에는 각 인증서 요청과 CA 데이터베이스에서 발급된 인증서의 기록 저장이 포함됩니다. 대량의 요청이 지속되면 CA 데이터베이스 성장률이 높아지며, 모니터링하지 않을 경우 사용 가능한 디스크 공간을 모두 소비할 수 있습니다. 비영구 인증서 처리를 사용하도록 설정하면 CA 데이터베이스 성장률과 데이터베이스 관리 작업의 빈도를 줄이는 데 도움이 됩니다.

사전 요구 사항

- Windows Server 2008 R2, Windows Server 2012 R2, Windows Server 2016 또는 Windows Server 2019 가상 시스템을 생성합니다.
- 가상 시스템이 Horizon 7 배포를 위한 Active Directory 도메인에 속하는지 확인합니다.
- IPv4 환경을 사용하고 있는지 확인합니다. 이 기능은 현재 IPv6 환경에서 지원되지 않습니다.
- 시스템에 고정 IP 주소가 있는지 확인합니다.

절차

- 1 가상 시스템 운영 체제에 관리자로 로그인하여 서버 관리자를 시작합니다.
- 2 역할 추가에 사용할 설정을 선택합니다.

운영 체제	선택
■ Windows Server 2012 R2	a 역할 및 기능 추가를 선택합니다.
■ Windows Server 2016	b 설치 유형 선택 페이지에서 역할 기반 또는 기능 기반 설치 를 선택합니다.
■ Windows Server 2019	c 대상 서버 선택 페이지에서 서버를 선택합니다.
Windows Server 2008 R2	a 탐색 트리에서 역할 을 선택합니다.
	b 역할 추가 를 클릭하여 역할 추가 마법사를 시작합니다.

- 3 서버 역할 선택 페이지에서 **Active Directory 인증서 서비스**를 선택합니다.
- 4 역할 및 기능 추가 마법사에서 **기능 추가**를 클릭하고 **관리 도구 포함** 확인란을 선택된 상태로 둡니다.
- 5 기능 선택 페이지에서 기본값을 그대로 사용합니다.
- 6 역할 서비스 선택 페이지에서 **CA(인증 기관)**를 선택합니다.

- 7 표시되는 메시지에 따라 설치를 완료합니다.
- 8 설치가 완료되면 설치 진행 페이지에서 **대상 서버에 Active Directory 인증서 서비스 구성** 링크를 클릭하여 AD CS 구성 마법사를 엽니다.
- 9 자격 증명 페이지에서 **다음**을 클릭하고 다음 표에 설명된 대로 AD CS 구성 마법사 페이지를 완료합니다.

옵션	조치
역할 서비스	CA(인증 기관)를 선택한 후, 구성이 아닌 다음 을 클릭합니다.
설정 유형	Enterprise CA를 선택합니다.
CA 유형	루트 CA 또는 종속 CA를 선택합니다. 2계층 PKI 배포를 선호하는 기업도 있습니다. 자세한 내용은 http://social.technet.microsoft.com/wiki/contents/articles/15037.ad-cs-step-by-step-guide-two-tier-pki-hierarchy-deployment.aspx 의 내용을 참조하십시오.
개인 키	새 개인 키 만들기를 선택합니다.
CA의 암호화	해시 알고리즘으로는 SHA1, SHA256, SHA384 또는 SHA512를 선택할 수 있습니다. 키 길이로는 1024, 2048, 3072 또는 4096을 선택할 수 있습니다. VMware에서는 최소 SHA256 및 2048 키를 권장합니다.
CA 이름	기본값을 수락하거나 이름을 변경합니다.
유효 기간	기본값인 5년을 수락합니다.
인증서 데이터베이스	기본값을 수락합니다.

- 10 확인 페이지에서 **구성**을 클릭하고 마법사가 구성에 성공한 것을 보고하면 마법사를 닫습니다.
- 11 명령 프롬프트를 열고 다음 명령을 입력하여 비영구 인증서 처리를 위한 CA를 구성합니다.

```
certutil -setreg DBFlags +DBFLAGS_ENABLEVOLATILEREQUESTS
```

- 12 CA에서 오프라인 CRL(인증서 해지 목록) 오류를 무시하려면 다음 명령을 입력합니다.

```
certutil -setreg ca\CRLFlags +CRLF_REVCHECK_IGNORE_OFFLINE
```

이 플래그가 필요한 이유는 True SSO에서 사용하는 루트 인증서가 보통 오프라인이고, 따라서 예정대로 해지 확인이 실패하기 때문입니다.

- 13 다음 명령을 입력하여 서비스를 다시 시작합니다.

```
sc stop certsvc
sc start certsvc
```

다음에 수행할 작업

인증서 템플릿을 생성합니다. True SSO에 사용하는 인증서 템플릿 만들기의 내용을 참조하십시오.

True SSO에 사용하는 인증서 템플릿 만들기

일시적인 인증서를 발급하는 데 사용할 수 있는 인증서 템플릿을 만들어야 하며, 도메인에 있는 컴퓨터 중에 이러한 유형의 인증서를 요청할 수 있는 컴퓨터를 지정해야 합니다.

둘 이상의 인증서 템플릿을 생성할 수 있습니다. 도메인당 하나의 템플릿만 구성할 수 있지만 여러 도메인에 걸쳐 템플릿을 공유할 수 있습니다. 예를 들어, 3개의 도메인을 포함하는 Active Directory 포리스트가 있고 세 개의 도메인 모두에 대해 True SSO를 사용하려는 경우 1개, 2개 또는 3개의 템플릿을 구성하도록 선택할 수 있습니다. 모든 도메인이 동일한 템플릿을 공유할 수도 있고 도메인마다 다른 템플릿을 사용할 수도 있습니다.

사전 요구 사항

- 이 절차에 설명된 템플릿을 만드는 데 사용할 Enterprise CA가 있는지 확인합니다. [Enterprise CA 설정](#)의 내용을 참조하십시오.
- 스마트 카드 인증을 위해 Active Directory를 준비했는지 확인합니다. 자세한 내용은 Horizon 7 설치 문서를 참조하십시오.
- 도메인에 보안 그룹을 만들고, 등록 서버에 포리스트를 만들고, 등록 서버의 컴퓨터 계정을 그 그룹에 추가합니다.

절차

- 1 True SSO를 구성하려면 CA(인증 기관)에 사용하는 시스템에서 운영 체제에 관리자로 로그인하고 **관리 도구 > CA(인증 기관)**로 이동합니다.
 - a 왼쪽 창에서 트리를 확장하고 **인증서 템플릿**을 마우스 오른쪽 버튼으로 클릭한 다음 **관리**를 선택합니다.
 - b **스마트 카드 로그인** 템플릿을 마우스 오른쪽 버튼으로 클릭하고 **복제**를 선택합니다.

c 다음 탭에서 다음 사항을 변경합니다.

탭	조치
호환성 탭	<ul style="list-style-type: none"> CA(인증 기관)로 Windows Server 2008 R2를 선택합니다. 인증 수신자로 Windows 7/Windows Server 2008 R2를 선택합니다.
일반 탭	<ul style="list-style-type: none"> 템플릿 디스플레이 이름을 True SSO로 변경합니다. 유효 기간을 일반적인 업무일 기간, 즉 사용자가 시스템에서 로그인을 유지하는 기간으로 변경합니다. <p>사용자가 로그인해 있는 동안 네트워크 리소스에 대한 액세스가 끊어지지 않도록, 유효 기간은 사용자 도메인의 Kerberos TGT 갱신 시간보다 길어야 합니다.</p> <p>(티켓의 기본 최대 수명은 10시간입니다. 기본 도메인 정책을 찾으려면 컴퓨터 구성 > 정책 > Windows 설정 > 보안 설정 > 계정 정책 > Kerberos 정책:사용자 티켓 최대 수명으로 이동할 수 있습니다.)</p> <ul style="list-style-type: none"> 갱신 기간을 유효 기간의 50%-75%로 변경합니다.
요청 처리 탭	<ul style="list-style-type: none"> 목적에서 서명 및 스마트 카드 로그인을 선택합니다. 스마트 카드를 자동 갱신하려면...을 선택합니다.
암호화 탭	<ul style="list-style-type: none"> 제공자 범주에서 키 저장소 제공자를 선택합니다. 알고리즘 이름에서 RSA를 선택합니다.
서버 탭	<p>CA 데이터베이스에 인증서 및 요청 저장 안 함을 선택합니다.</p> <p>중요 발급된 인증서에 해지 정보를 포함하지 않음을 선택 취소합니다. (첫 번째 상자를 선택하면 이 상자가 선택되며, 선택 취소해서 표시를 지워야 합니다.)</p>
발급 요구 사항 탭	<ul style="list-style-type: none"> 권한 부여 수를 선택하고 상자에 1을 입력합니다. 정책 유형에서 애플리케이션 정책을 선택하고 정책을 인증서 요청 에이전트로 설정합니다. 등록에 다음 필요에서 유효한 기존 인증서를 선택합니다.
보안 탭	<p>등록 서버 컴퓨터 계정에 생성한 보안 그룹에 대해 전제 조건에 설명된 대로 읽기, 등록 권한을 제공합니다.</p> <ol style="list-style-type: none"> 추가를 클릭합니다. 인증서에 대해 등록을 허용할 컴퓨터를 지정합니다. 이러한 컴퓨터에 대해 적절한 확인란을 선택하여 컴퓨터에 읽기, 등록 권한을 제공합니다.

d 새 템플릿 대화 상자의 속성에서 **확인**을 클릭합니다.

e 인증서 템플릿 콘솔 창을 닫습니다.

f **인증서 템플릿**을 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기 > 발급할 인증서 템플릿**을 선택합니다.

참고 이 템플릿을 기반으로 인증서를 발급하려는 모든 CA(인증 기관)에 대해 이 단계가 필요합니다.

g 인증서 템플릿 사용 창에서 방금 만든 템플릿을 선택하고(예: **True SSO 템플릿**) **확인**을 클릭합니다.

2 등록 에이전트 컴퓨터를 구성하려면 CA(인증 기관)에 사용하는 시스템에서 운영 체제에 관리자로 로그인하고 **관리 도구 > CA(인증 기관)**로 이동합니다.

a 왼쪽 창에서 트리를 확장하고 **인증서 템플릿**을 마우스 오른쪽 버튼으로 클릭한 다음 **관리**를 선택합니다.

b 등록 에이전트 컴퓨터 템플릿을 찾아서 연 다음 **보안** 탭에서 다음과 같이 변경합니다.

등록 서버 컴퓨터 계정에 생성한 보안 그룹에 대해 전제 조건에 설명된 대로 읽기, 등록 권한을 제공합니다.

1 **추가**를 클릭합니다.

2 인증서에 대해 등록을 허용할 컴퓨터를 지정합니다.

3 이러한 컴퓨터에 대해 적절한 확인란을 선택하여 컴퓨터에 읽기, 등록 권한을 제공합니다.

c **인증서 템플릿**을 마우스 오른쪽 버튼으로 클릭하고 **새로 만들기 > 발급할 인증서 템플릿**을 선택합니다.

참고 이 템플릿을 기반으로 인증서를 발급하려는 모든 CA(인증 기관)에 대해 이 단계가 필요합니다.

d 인증서 템플릿 사용 창에서 **등록 에이전트 컴퓨터**를 선택하고 **확인**을 클릭합니다.

다음에 수행할 작업

등록 서비스를 생성합니다. **등록 서버 설치 및 설정**의 내용을 참조하십시오.

등록 서버 설치 및 설정

연결 서버 설치 관리자를 실행하고 Horizon 7 등록 서버 옵션을 사용하여 등록 서버를 설치할 수 있습니다. 등록 서버에서는 지정된 사용자에게 대해 일시적인 인증서를 요청합니다. 이러한 단기 인증서는 True SSO에서 사용자에게 Active Directory 자격 증명을 요청하는 메시지가 표시되지 않도록 하기 위해 인증 목적으로 사용하는 메커니즘입니다.

등록 서버를 하나 이상 설치 및 설정해야 하며, 등록 서버를 View 연결 서버와 동일한 호스트에 설치할 수는 없습니다. VMware는 페일오버와 로드 밸런싱을 위해 두 개의 등록 서버를 둘 것을 권장합니다. 등록 서버가 두 개인 경우에는 기본적으로 하나는 기본 서버로, 다른 하나는 페일오버 서버로 사용합니다. 그러나 연결 서버에서 두 등록 서버에 번갈아 인증서 요청을 보내도록 이 기본값을 변경할 수 있습니다.

Enterprise CA를 호스팅하는 동일한 시스템에 등록 서버를 설치하면 등록 서버에서 로컬 CA를 기본으로 사용하도록 구성할 수 있습니다. 최고의 성능을 위한 VMware 권장 사항은 로컬 CA를 기본적으로 사용하도록 하는 구성과 등록 서버를 로드 밸런싱하도록 하는 구성을 결합하는 것입니다. 따라서, 인증서 요청이 도착하면 연결 서버에서 대체 등록 서버를 사용하며, 각 등록 서버에서 로컬 CA를 사용하여 요청을 서비스합니다. 사용할 구성 설정에 대한 자세한 내용은 **등록 서버 구성 설정** 및 **연결 서버 구성 설정**을 참조하십시오.

사전 요구 사항

- 메모리가 4GB 이상인 Windows Server 2008 R2, Windows Server 2012 R2 또는 Windows Server 2016 가상 시스템을 만들거나 Enterprise CA를 호스팅하는 가상 시스템을 사용합니다. 도메인 컨트롤러 시스템은 사용하지 마십시오.
- View 연결 서버, View Composer, 보안 서버, Horizon Client, View Agent, Horizon Agent를 포함한 다른 View 구성 요소가 가상 시스템에 설치되어 있지 않은지 확인합니다.
- 가상 시스템이 Horizon 7 배포를 위한 Active Directory 도메인에 속하는지 확인합니다.
- IPv4 환경을 사용하고 있는지 확인합니다. 이 기능은 현재 IPv6 환경에서 지원되지 않습니다.
- VMware에서는 시스템에 고정 IP 주소를 지정할 것을 권장합니다.
- 관리자 권한이 있는 도메인 사용자로 운영 체제에 로그인할 수 있는지 확인합니다. 설치 관리자를 실행하려면 관리자로 로그인해야 합니다.

절차

- 1 등록 서버로 사용할 시스템에서 MMC에 인증서 스냅인 추가:
 - a MMC 콘솔을 열고 **파일 > 스냅인 추가/제거**를 선택합니다.
 - b **사용 가능한 스냅인**에서 **인증서**를 선택하고 **추가**를 클릭합니다.
 - c 인증서 스냅인 창에서 **컴퓨터 계정**을 선택하고 **다음**을 클릭한 다음 **마침**을 클릭합니다.
 - d 스냅인 추가 또는 제거 창에서 **확인**을 클릭합니다.
- 2 등록 에이전트 인증서 발급:
 - a 인증서 콘솔에서 콘솔 루트 트리를 확장하고 **개인 설정** 폴더를 마우스 오른쪽 버튼으로 클릭하고 **모든 작업 > 새 인증서 요청**을 선택합니다.
 - b 인증서 등록 마법사에서 인증서 요청 페이지로 이동할 때까지 기본값을 수락합니다.
 - c 인증서 요청 페이지에서 **등록 에이전트(컴퓨터)** 확인란을 선택하고 **등록**을 클릭합니다.
 - d 나머지 마법사 페이지에서 기본값을 수락하고 마지막 페이지에서 **마침**을 클릭합니다.

MMC 콘솔에서 **개인 설정** 폴더를 확장하고 왼쪽 창에서 **인증서**를 선택하면 오른쪽 창에 새 인증서가 나열되는 것을 볼 수 있습니다.

- 3 등록 서버 설치:
 - a VMware 다운로드 사이트(<https://my.vmware.com/web/vmware/downloads>)에서 View 연결 서버 설치 관리자 파일을 다운로드합니다.

Desktop & End-User Computing에서 View 연결 서버가 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

설치 관리자 파일 이름은 VMware-viewconnectionserver-x86_64-y.y.y-xxxxxx.exe입니다. 여기서 xxxxxx는 빌드 번호이며 y.y.y는 버전 번호입니다.
 - b 설치 관리자 파일을 두 번 클릭하여 마법사를 시작하고 프롬프트에 따라 설치 옵션 페이지로 이동합니다.

- c [설치 옵션] 페이지에서 **Horizon 7 등록 서버**를 선택하고 등록 서버 인스턴스에 대한 인증 모드를 선택한 후 **다음**을 클릭합니다.

옵션	설명
Horizon 7	Horizon 7 환경에 대한 인증 모드를 구성합니다.
Horizon Cloud	Horizon Cloud 환경에 대한 인증 모드를 구성합니다.

- d 표시되는 메시지에 따라 설치를 완료합니다.

등록 서버가 작동하려면 포트 32111(TCP)에서 수신 연결을 사용하도록 설정해야 합니다. 설치 관리자에서는 설치하는 동안 기본적으로 이 포트를 엽니다.

다음에 수행할 작업

- Enterprise CA를 호스팅하는 동일한 시스템에 등록 서버를 설치했다면 등록 서버에서 로컬 CA를 기본으로 사용하도록 구성합니다. [등록 서버 구성 설정](#)의 내용을 참조하십시오. 선택적으로 두 개 이상의 등록 서버를 설치 및 설정하는 경우, 등록 서버 간의 로드 밸런싱을 사용하도록 연결 서버를 구성합니다. [연결 서버 구성 설정](#)을 참조하십시오.
- 연결 서버와 등록 서버를 연결합니다. [등록 서비스 클라이언트 인증서 내보내기](#)를 참조하십시오.

등록 서비스 클라이언트 인증서 내보내기

연결을 위해, MMC 인증서 스냅인을 사용하여 자동으로 생성되고 자체 서명된 등록 서비스 클라이언트 인증서를 클러스터에 있는 한 연결 서버에서 내보낼 수 있습니다. 연결 서버가 등록 서버에서 제공하는 등록 서비스의 클라이언트이기 때문에 이 인증서를 클라이언트 인증서라고 합니다.

등록 서버에서 Active Directory 사용자에게 대해 수명이 짧은 인증서를 발급하라는 메시지를 표시할 경우, 등록 서버에서 VMware Horizon 연결 서버를 신뢰해야 합니다. 따라서 VMware Horizon 연결 서버 또는 포트를 등록 서버와 연결해야 합니다.

Horizon 7 이상 연결 서버가 설치되어 있을 때 VMware Horizon 연결 서버 서비스가 시작되면 등록 서비스 클라이언트 인증서가 자동으로 생성됩니다. 인증서는 View LDAP를 통해 나중에 클러스터에 추가되는 다른 Horizon 7 연결 서버에 배포됩니다. 인증서는 그 후에 컴퓨터의 Windows 인증서 저장소에 있는 사용자 지정 컨테이너(VMware Horizon View Certificates\WCertificates)에 저장됩니다.

사전 요구 사항

Horizon 7 이상 연결 서버가 설치되어 있는지 확인합니다. 설치 지침은 Horizon 7 설치를 참조하십시오. 업그레이드 지침은 Horizon 7 업그레이드를 참조하십시오.

중요 고객은 연결 서버에서 생성되고 자체 서명된 인증서를 사용하지 않고 자신의 인증서를 사용할 수 있습니다. 그러려면 연결 서버 시스템의 Windows 인증서 저장소에 있는 사용자 지정 컨테이너(VMware Horizon View Certificates\WCertificates)에 기본 인증서(및 관련 개인 키)를 넣습니다. 그리고 나면 인증서의 대화명으로 **vdm.ec.new**를 설정한 후 서버를 다시 시작해야 합니다. 클러스터에 있는 다른 서버가 LDAP에서 이 인증서를 가져옵니다. 그 후에 이 절차의 단계를 수행할 수 있습니다.

절차

- 클러스터에 있는 연결 서버 시스템 중 하나에서 인증서 스냅인을 다음과 같이 MMC에 추가합니다.
 - MMC 콘솔을 열고 **파일 > 스냅인 추가/제거**를 선택합니다.
 - 사용 가능한 스냅인**에서 **인증서**를 선택하고 **추가**를 클릭합니다.
 - 인증서 스냅인 창에서 **컴퓨터 계정**을 선택하고 **다음**을 클릭한 다음 **마침**을 클릭합니다.
 - 스냅인 추가 또는 제거 창에서 **확인**을 클릭합니다.
- MMC 콘솔의 왼쪽 창에서 **VMware Horizon View 인증서** 폴더를 확장하고 **인증서** 폴더를 선택합니다.
- 오른쪽 창에서 대화명이 **vdm.ec**인 인증서 파일을 마우스 오른쪽 버튼으로 클릭하고 **모든 작업 > 내보내기**를 선택합니다.
- 인증서 내보내기 마법사에서 기본값을 수락합니다. 여기에는 **아니요, 개인 키를 내보내지 않습니다** 라디오 버튼을 선택된 채로 두는 것이 포함됩니다.
- 파일 이름을 입력하라는 메시지가 표시되면 등록 서비스 클라이언트 인증서에 **EnrollClient**와 같은 파일 이름을 입력하고 메시지에 따라 인증서 내보내기를 마칩니다.

다음에 수행할 작업

등록 서버에 인증서를 가져옵니다. [등록 서버로 등록 서비스 클라이언트 인증서 가져오기](#)의 내용을 참조하십시오.

등록 서버로 등록 서비스 클라이언트 인증서 가져오기

연결 프로세스를 완료하려면 MMC 인증서 스냅인을 사용하여 등록 서비스 클라이언트 인증서를 등록 서버로 가져옵니다. 이 절차는 모든 등록 서버에서 수행해야 합니다.

사전 요구 사항

- Horizon 7 이상의 등록 서버가 있는지 확인합니다. [등록 서버 설치 및 설정](#)의 내용을 참조하십시오.
- 가져올 올바른 인증서 파일이 있는지 확인합니다. 사용자의 자체 인증서를 사용할 수도 있고, [등록 서비스 클라이언트 인증서 내보내기](#)에 설명된 대로 클러스터의 한 연결 서버에서 자동으로 생성되고 자체 서명된 등록 서비스 클라이언트 인증서를 사용할 수도 있습니다.

중요 사용자의 자체 인증서를 연결에 사용하려면 연결 서버 시스템에서 Windows 인증서 저장소의 사용자 지정 컨테이너(VMware Horizon View Certificates\WCertificates)에 원하는 인증서(및 관련 개인 키)를 삽입합니다. 그리고 나면 인증서의 대화명으로 **vdm.ec.new**를 설정한 후 서버를 다시 시작해야 합니다. 클러스터에 있는 다른 서버가 LDAP에서 이 인증서를 가져옵니다. 그 후에 이 절차의 단계를 수행할 수 있습니다.

사용자의 자체 클라이언트 인증서가 있는 경우 등록 서버로 복사해야 할 인증서는 클라이언트 인증서 생성에 사용되는 루트 인증서입니다.

절차

1 적절한 인증서 파일을 등록 서버 시스템에 복사합니다.

자동으로 생성된 인증서를 사용하려면 연결 서버에서 등록 서비스 클라이언트 인증서를 복사합니다. 사용자의 자체 인증서를 사용하려면 클라이언트 인증서 생성에 사용된 루트 인증서를 복사합니다.

2 등록 서버에서 인증서 스냅인을 MMC에 추가합니다.

- a MMC 콘솔을 열고 **파일 > 스냅인 추가/제거**를 선택합니다.
- b **사용 가능한 스냅인**에서 **인증서**를 선택하고 **추가**를 클릭합니다.
- c 인증서 스냅인 창에서 **컴퓨터 계정**을 선택하고 **다음**을 클릭한 다음 **마침**을 클릭합니다.
- d 스냅인 추가 또는 제거 창에서 **확인**을 클릭합니다.

3 MMC 콘솔의 왼쪽 창에서 **VMware Horizon View 등록 서버의 신뢰할 수 있는 루트** 폴더를 마우스 오른쪽 버튼으로 클릭하고 **모든 작업 > 가져오기**를 선택합니다.

4 인증서 가져오기 마법사에서 프롬프트에 따라 **EnrollClient** 인증서 파일로 이동하여 파일을 엽니다.

5 프롬프트에 따라 기본값을 수락하고 인증서 가져오기를 마칩니다.

6 가져온 인증서를 마우스 오른쪽 버튼으로 클릭하고 **vdm.ec**(등록 클라이언트 인증서의 경우)와 같은 대화명을 추가합니다.

VMware에서는 Horizon 7 클러스터를 나타내는 대화명을 사용할 것을 권장하지만, 클라이언트 인증서를 쉽게 식별하는 데 도움이 되는 모든 이름을 사용할 수 있습니다.

다음에 수행할 작업

VMware Identity Manager에 인증을 위임할 때 사용되는 SAML 인증자를 구성합니다. [SAML 인증이 True SSO에서 작동하도록 구성](#)의 내용을 참조하십시오.

SAML 인증이 True SSO에서 작동하도록 구성

Horizon 7에 도입된 True SSO 기능을 사용하면, 사용자가 스마트 카드, RADIUS 또는 RSA SecurID 인증을 사용하여 VMware Identity Manager 2.6 이상 릴리스에 로그인할 수 있으며 그 후에는 원격 데스크톱이나 애플리케이션을 처음으로 실행해도 Active Directory 자격 증명을 요청하는 메시지가 표시되지 않습니다.

초기 릴리스에서 SSO(Single Sign-On)는 사용자가 이전에 Active Directory 자격 증명을 사용하여 인증하지 않은 경우 처음으로 원격 데스크톱이나 게시된 애플리케이션을 실행하면 Active Directory 자격 증명을 요청하는 메시지를 표시하는 방식으로 작동되었습니다. 그러면 이후 실행에서 사용자가 자격 증명을 다시 입력할 필요가 없도록 자격 증명이 캐시됩니다. True SSO를 사용하면 AD 자격 증명 대신 단기 인증서가 생성 및 사용됩니다.

VMware Identity Manager에 대해 SAML 인증을 구성하는 프로세스는 변경되지 않았지만, True SSO에 대해 단계 하나가 더 추가되었습니다. VMware Identity Manager를 암호 팝업이 표시되지 않도록 구성해야 합니다.

참고 배포에 둘 이상의 연결 서버 인스턴스가 포함된 경우 SAML 인증자를 각 인스턴스에 연결해야 합니다.

사전 요구 사항

- Single Sign-On이 전역 설정으로 사용되도록 설정되어 있는지 확인합니다. Horizon Administrator에서 **구성 > 전역 설정**을 선택하고 **SSO(Single Sign-On)**가 **사용**으로 설정되어 있는지 확인합니다.
- VMware Identity Manager가 설치 및 구성되어 있는지 확인합니다.
<https://docs.vmware.com/kr/VMware-Identity-Manager/index.html>에 있는 VMware Identity Manager 설명서를 참조하십시오.
- SAML 서버 인증서의 서명 CA에 대한 루트 인증서가 연결 서버 호스트에 설치되어 있는지 확인합니다. 자체 서명된 인증서를 사용하도록 SAML 인증자를 구성하지 않는 것이 좋습니다.
Horizon 7 설치 문서의 "Horizon 7 Server를 위한 SSL 인증서 구성" 장에서 "Windows 인증서 저장소에 루트 인증서 및 중간 인증서 가져오기" 항목을 참조하십시오.
- VMware Identity Manager 서버 인스턴스의 FQDN을 기록해 둡니다.

절차

- 1 Horizon Administrator에서 **구성 > 서버**를 선택합니다.
- 2 **연결 서버** 탭에서 SAML 인증자에 연결할 서버 인스턴스를 선택하고 **편집**을 클릭합니다.
- 3 **인증** 탭의 **VMware Horizon(SAML 2.0 인증자)**에 **인증 위임** 드롭다운 메뉴에서 **허용** 또는 **필수**를 선택합니다.

각자의 요구 사항에 따라 다른 SAML 인증 설정을 가지도록 배포 내의 각 연결 서버 인스턴스를 구성할 수 있습니다.

- 4 **SAML 인증자 관리**를 클릭하고 **추가**를 클릭합니다.
- 5 SAML 2.0 인증자 추가 대화 상자에서 SAML 인증자를 구성합니다.

옵션	설명
레이블	VMware Identity Manager 서버 인스턴스의 FQDN을 사용할 수 있습니다.
설명	(선택 사항) VMware Identity Manager 서버 인스턴스의 FQDN을 사용할 수 있습니다.

옵션	설명
메타데이터 URL	SAML ID 제공자와 Horizon 연결 서버 인스턴스 간에 SAML 정보를 교환하기 위해 필요한 모든 정보를 검색하기 위한 URL입니다. URL <code>https://<YOUR HORIZON SERVER NAME>/SAAS/API/1.0/GET/metadata/idp.xml</code> 에서 <YOUR HORIZON SERVER NAME> 을 클릭하고 VMware Identity Manager 서버 인스턴스의 FQDN으로 바꿉니다.
관리 URL	SAML ID 공급자의 관리 콘솔에 액세스하기 위한 URL입니다 (VMware Identity Manager 인스턴스). 이 URL의 형식은 <code>https://<Identity-Manager-FQDN>:8443</code> 입니다.

6 확인을 클릭하여 SAML 인증자 구성을 저장합니다.

올바른 정보를 제공한 경우 자체 서명된 인증서를 수락하거나(권장하지 않음) Horizon 7 및 VMware Identity Manager의 신뢰할 수 있는 인증서를 사용해야 합니다.

SAML 2.0 인증자 드롭다운 메뉴에 이제 선택한 인증자로 설정되어 있는 새로 생성된 인증자가 표시됩니다.

7 Horizon Administrator 대시보드의 시스템 상태 섹션에서 기타 구성 요소 > SAML 2.0 인증자를 선택하고 추가한 SAML 인증자를 선택한 다음 세부 정보를 확인합니다.

구성에 성공한 경우 인증자의 상태는 녹색입니다. 인증서를 신뢰할 수 없는 경우, VMware Identity Manager 서비스를 사용할 수 없는 경우 또는 메타데이터 URL이 잘못된 경우 인증자의 상태가 빨간색으로 표시될 수 있습니다. 인증서를 신뢰할 수 없는 경우 **확인**을 클릭하여 인증서를 검증 및 수락할 수 있습니다.

8 VMware Identity Manager 관리 콘솔에 로그인하고 View 풀 페이지로 이동한 다음 암호 팝업을 표시하지 않음 확인란을 선택합니다.

다음에 수행할 작업

- 원격 세션이 24시간 후에 종료되지 않도록 연결 서버 메타데이터의 만료 기간을 연장합니다. [연결 서버에서 서비스 제공자 메타데이터의 만료 기간 변경](#)의 내용을 참조하십시오.
- `vdmutl` 명령줄 인터페이스를 사용하여 연결 서버에 True SSO를 구성합니다. [True SSO에 대한 Horizon 연결 서버 구성](#)의 내용을 참조하십시오.

SAML 인증의 작동 방식에 대한 자세한 내용은 [SAML 인증 사용](#)을 참조하십시오.

True SSO에 대한 Horizon 연결 서버 구성

`vdmutl` 명령줄 인터페이스를 사용하여 True SSO를 구성하거나 사용 또는 사용 안 함으로 설정할 수 있습니다.

이 절차는 클러스터의 연결 서버 중 하나에서만 수행하면 됩니다.

중요 이 절차에서는 True SSO 사용에 필요한 명령만 사용합니다. True SSO 구성 관리에 사용할 수 있는 모든 구성 옵션의 목록과 각 옵션에 대한 설명은 [True SSO 구성을 위한 명령줄 참조](#)를 참조하십시오.

사전 요구 사항

- 관리자 역할을 가진 사용자로 명령을 실행할 수 있는지 확인합니다. Horizon Administrator를 사용하여 사용자에게 관리자 역할을 할당할 수 있습니다. [장6역할 기반 위임된 관리 구성](#)의 내용을 참조하십시오.
- 다음 서버에 대해 정규화된 도메인 이름(FQDN)이 있는지 확인합니다.
 - 연결 서버
 - 등록 서버
 자세한 내용은 [등록 서버 설치 및 설정](#)의 내용을 참조하십시오.
- Enterprise CA(인증 기관)
 - 자세한 내용은 [Enterprise CA 설정](#)의 내용을 참조하십시오.
- 도메인의 Netbios 이름 또는 FQDN을 가지고 있는지 확인합니다.
- 인증서 템플릿을 만들었는지 확인합니다. [True SSO에 사용하는 인증서 템플릿 만들기](#)의 내용을 참조하십시오.
- SAML 인증자를 만들어 VMware Identity Manager에 인증을 위임했는지 확인합니다. [SAML 인증이 True SSO에서 작동하도록 구성](#)의 내용을 참조하십시오.

절차

- 1 클러스터의 연결 서버에서 명령 프롬프트를 열고 명령을 입력하여 등록 서버를 추가합니다.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --environment --add --enrollmentServer enroll-server-fqdn
```

등록 서버가 전역 목록에 추가됩니다.

- 2 명령을 입력하여 해당 등록 서버의 정보를 나열합니다.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn
```

출력에는 포리스트 이름, 등록 서버의 인증서가 유효한지 여부, 사용할 수 있는 인증서 템플릿의 이름과 세부 정보, 인증 기관의 일반 이름이 표시됩니다. 등록 서버에서 어떤 도메인에 연결할 수 있는지 구성하려면 등록 서버에서 Windows 레지스트리 설정을 사용할 수 있습니다. 기본값은 신뢰하는 모든 도메인에 연결하는 것입니다.

중요 다음 단계에서는 인증 기관의 일반 이름을 지정해야 합니다.

- 3 명령을 입력하여 구성 정보가 있는 True SSO 커넥터를 만들고 커넥터를 사용하도록 설정합니다.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --create --connector --domain domain-fqdn --template TrueSSO-template-name --primaryEnrollmentServer enroll-server-fqdn --certificateServer ca-common-name --mode enabled
```

이 명령에서 TrueSSO-template-name은 이전 단계의 출력에 표시된 템플릿의 이름이고, ca-common-name은 그 출력에 표시된 Enterprise 인증 기관의 일반 이름입니다.

True SSO 커넥터는 지정한 도메인의 풀 또는 클러스터에서 사용하도록 설정됩니다. 풀 수준에서 True SSO를 사용하지 않도록 설정하려면 vdmUtil --certsso --edit --connector <domain> --mode disabled를 실행합니다. 개별 가상 시스템에서 True SSO를 사용하지 않도록 설정하는 경우에는 GPO(vdm_agent.adm)를 사용할 수 있습니다.

- 4 명령을 입력하여 어떤 SAML 인증자를 사용할 수 있는지 확인합니다.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --list --authenticator
```

인증자는 Horizon Administrator를 사용하여 VMware Identity Manager와 연결 서버 사이에 SAML 인증을 구성할 때 생성됩니다.

출력에는 인증자의 이름과 True SSO 사용 여부가 표시됩니다.

중요 다음 단계에서는 인증자 이름을 지정해야 합니다.

- 5 명령을 입력하여 인증자에서 True SSO 모드를 사용하도록 설정합니다.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --authenticator --edit --name authenticator-fqdn --truessoMode {ENABLED|ALWAYS}
```

--truessoMode의 경우, 사용자가 VMware Identity Manager에 로그인할 때 암호가 제공되지 않은 경우에는 ENABLED를 사용합니다. 이 경우 암호를 사용하고 캐시하면 시스템에서 암호를 사용합니다. 사용자가 VMware Identity Manager에 로그인할 때 암호를 제공하지 않아도 True SSO를 사용할 수 있게 하려면 --truessoMode를 ALWAYS로 설정합니다.

다음에 수행할 작업

Horizon Administrator에서 True SSO 구성의 상태를 확인합니다. 자세한 내용은 [시스템 상태 대시보드를 사용하여 True SSO와 관련된 문제 해결](#)의 내용을 참조하십시오.

고급 옵션을 구성하려면 적절한 시스템에서 Windows 고급 설정을 사용합니다. [True SSO에 대한 고급 구성 설정](#)의 내용을 참조하십시오.

True SSO 구성을 위한 명령줄 참조

vdmutil 명령줄 인터페이스를 사용하여 True SSO 기능을 구성하고 관리할 수 있습니다.

유틸리티의 위치

기본적으로 vdmutil 명령 실행 파일의 경로는 C:\Program Files\VMware\VMware View\ServerTools\Wbin입니다. 명령줄에 경로를 입력하지 않으려면 PATH 환경 변수에 경로를 추가하십시오.

구문 및 인증

Windows 명령 프롬프트에서 다음 vdmutil 명령 형식을 사용합니다.

```
vdmutil 인증 옵션 --truesso 추가 옵션 및 인수
```

사용할 수 있는 추가 옵션은 명령 옵션에 따라 다릅니다. 이 항목에서는 True SSO(--truesso) 구성을 위한 옵션을 집중적으로 다룹니다. 다음은 True SSO에 대해 구성된 커넥터를 나열하는 명령의 예입니다.

```
vdmUtil --authAs admin-role-user --authDomain domain-name --authPassword admin-user-password --truesso --list --connector
```

vdmutil 명령에는 인증에 사용할 사용자 이름, 도메인 및 암호를 지정하는 인증 옵션이 있습니다.

표 5-1. vdmutil 명령 인증 옵션

옵션	설명
--authAs	Horizon 7 관리자 사용자의 이름입니다. domain\username 또는 UPN(사용자 계정 이름) 형식을 사용하지 마십시오.
--authDomain	--authAs 옵션에 지정된 Horizon 7 관리자의 정규화된 도메인 이름 또는 Netbios 이름입니다.
--authPassword	--authAs 옵션에 지정된 Horizon 7 관리자 사용자의 암호입니다. 암호 대신 "*"를 입력하면 vdmutil 명령이 암호를 묻는 메시지를 표시하고 명령줄에서 중요 암호를 명령 기록에 남기지 않습니다.

--help 및 --verbose를 제외한 모든 vdmutil 명령 옵션과 함께 인증 옵션을 사용해야 합니다.

명령 출력

vdmutil 명령은 작업이 성공하면 0을 반환하고 작업이 실패하면 0이 아닌 장애 관련 코드를 반환합니다. vdmutil 명령은 오류 메시지를 표준 오류로 기록합니다. 작업에서 출력을 생성하거나 자세한 정보 로깅이 --verbose 옵션을 사용하여 사용하도록 설정된 경우 vdmutil 명령은 출력을 표준 출력에 영어로 기록합니다.

등록 서버의 관리 명령

각 도메인에 등록 서버 하나를 추가해야 합니다. 두 번째 등록 서버를 추가한 후 나중에 그 서버를 백업으로 사용하도록 지정할 수도 있습니다.

읽기 쉽도록 하기 위해, 다음 표에 있는 옵션은 입력할 명령 전체를 표시하지 않습니다. 특정 작업에 관련된 옵션만 포함되었습니다. 예를 들어, 한 행에는 `--environment --list --enrollmentServers` 옵션이 표시되어 있는데, 실제로 입력하는 `vdmUtil` 명령에는 인증 옵션과 True SSO 구성을 지정하기 위한 옵션도 포함되어 있습니다.

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --truesso --environment --list --enrollmentServers
```

인증 옵션에 대한 자세한 내용은 [True SSO 구성을 위한 명령줄 참조](#)를 참조하십시오.

표 5-2. 등록 서버 관리를 위한 vdmutil truesso 명령 옵션

명령 및 옵션	설명
<code>--environment --add --enrollmentServer enroll-server-fqdn</code>	지정한 등록 서버를 환경에 추가하며, 여기서 <code>enroll-server-fqdn</code> 은 등록 서버의 FQDN입니다. 등록 서버가 이미 추가된 경우에는 이 명령을 실행해도 아무런 변화가 없습니다.
<code>--environment --remove --enrollmentServer enroll-server-fqdn</code>	지정한 등록 서버를 환경에서 제거하며, 여기서 <code>enroll-server-fqdn</code> 은 등록 서버의 FQDN입니다. 등록 서버가 이미 제거된 경우에는 이 명령을 실행해도 아무런 변화가 없습니다.
<code>--environment --list --enrollmentServers</code>	환경에 있는 모든 등록 서버의 FQDN을 나열합니다.
<code>--environment --list --enrollmentServer enroll-server-fqdn</code>	<p>등록 서버가 속한 도메인과 포리스트에서 신뢰하는 도메인 및 포리스트의 FQDN과 등록 인증서 상태(VALID 또는 INVALID)를 나열합니다. VALID는 등록 서버에 등록 에이전트 인증서가 설치된 것을 의미합니다. 상태가 INVALID가 되는 데는 다음과 같은 여러 가지 이유가 있을 수 있습니다.</p> <ul style="list-style-type: none"> ■ 인증서가 설치되지 않았습니다. ■ 인증서가 아직 유효하지 않거나 만료되었습니다. ■ 인증서가 신뢰할 수 있는 Enterprise CA에서 발급되지 않았습니다. ■ 개인 키를 사용할 수 없습니다. ■ 인증서가 손상되었습니다. <p>등록 서버의 로그 파일에서 INVALID 상태의 이유를 제공할 수 있습니다.</p>
<code>--environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn</code>	지정한 도메인의 등록 서버에 대해 사용 가능한 인증 기관의 CN(일반 이름)을 나열하고 True SSO에 사용할 수 있는 각 인증서 템플릿에 대해 이름, 최소 키 길이, 해시 알고리즘 정보를 제공합니다.

커넥터 관리 명령

각 도메인에 커넥터를 하나씩 만듭니다. 커넥터는 True SSO에 사용되는 매개 변수를 정의합니다.

읽기 쉽도록 하기 위해, 다음 표에 있는 옵션은 입력할 명령 전체를 표시하지 않습니다. 특정 작업에 관련된 옵션만 포함되었습니다. 예를 들어, 한 행에는 `--list --connector` 옵션이 표시되어 있는데, 실제로 입력하는 `vdmUtil` 명령에는 인증 옵션과 True SSO 구성을 지정하기 위한 옵션도 포함되어 있습니다.

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --truesso --list --connector
```


인증 옵션에 대한 자세한 내용은 [True SSO 구성을 위한 명령줄 참조](#)를 참조하십시오.

표 5-3. 커넥터 관리를 위한 vdmutil truesso 명령 옵션

옵션	설명
<code>--create --connector --domain domain-fqdn --template template-name --primaryEnrollmentServer enroll-server1-fqdn [--secondaryEnrollmentServer enroll-server2-fqdn] --certificateServer CA-common-name --mode {enabled disabled}</code>	<p>지정된 도메인에 대해 커넥터를 만들고 커넥터에서 다음 설정을 사용하도록 구성합니다.</p> <ul style="list-style-type: none"> ■ <code>template-name</code>은 사용할 인증서 템플릿의 이름입니다. ■ <code>enroll-server1-fqdn</code>은 사용할 기본 등록 서버의 FQDN입니다. ■ <code>enroll-server2-fqdn</code>은 사용할 보조 등록 서버의 FQDN입니다. 이 설정은 선택 사항입니다. ■ <code>CA-common-name</code>은 사용할 인증 기관의 일반 이름입니다. 쉼표로 구분된 CA 목록일 수도 있습니다. <p>특정 등록 서버에 대해 사용할 수 있는 인증서 템플릿과 CA(인증 기관)를 확인하려면 <code>vdmutil</code> 명령을</p> <p><code>--truesso --environment --list --enrollmentServer enroll-server-fqdn --domain domain-fqdn</code> 옵션과 함께 실행합니다.</p>
<code>--list --connector</code>	이미 커넥터가 생성된 도메인의 FQDN을 나열합니다.
<code>--list --connector --verbose</code>	<p>커넥터가 있는 모든 도메인을 나열하고 각 커넥터에 대해 다음 정보를 제공합니다.</p> <ul style="list-style-type: none"> ■ 기본 등록 서버 ■ 보조 등록 서버, 있는 경우 ■ 인증서 템플릿의 이름 ■ 커넥터의 사용 여부 ■ CA(인증 기관) 서버 또는 여러 서버(둘 이상인 경우)의 일반 이름입니다.
<code>--edit --connector domain-fqdn [--template template-name] [--mode {enabled disabled}] [--primaryEnrollmentServer enroll-server1-fqdn] [--secondaryEnrollmentServer enroll-server2-fqdn] [--certificateServer CA-common-name]</code>	<p><code>domain-fqdn</code>에서 지정한 도메인에 대해 생성된 커넥터를 사용하면 다음 설정을 변경할 수 있습니다.</p> <ul style="list-style-type: none"> ■ <code>template-name</code>은 사용할 인증서 템플릿의 이름입니다. ■ 이 모드는 <code>enabled</code> 또는 <code>disabled</code>일 수 있습니다. ■ <code>enroll-server1-fqdn</code>은 사용할 기본 등록 서버의 FQDN입니다. ■ <code>enroll-server2-fqdn</code>은 사용할 보조 등록 서버의 FQDN입니다. 이 설정은 선택 사항입니다. ■ <code>CA-common-name</code>은 사용할 인증 기관의 일반 이름입니다. 쉼표로 구분된 CA 목록일 수도 있습니다.
<code>--delete --connector domain-fqdn</code>	<code>domain-fqdn</code> 으로 지정된 도메인에 대해 생성된 커넥터를 삭제합니다.

인증자 관리 명령

인증자는 VMware Identity Manager Horizon 7과 연결 서버 사이에 SAML 인증을 구성할 때 생성됩니다. 관리 작업은 인증자의 True SSO를 사용 또는 사용 안 함으로 설정하는 것 뿐입니다.

읽기 쉽도록 하기 위해, 다음 표에 있는 옵션은 입력할 명령 전체를 표시하지 않습니다. 특정 작업에 관련된 옵션만 포함되었습니다. 예를 들어, 한 행에는 `--list --authenticator` 옵션이 표시되어 있는데, 실제로 입력하는 `vdmUtil` 명령에는 인증 옵션과 True SSO 구성을 지정하기 위한 옵션도 포함되어 있습니다.

```
vdmUtil --authAs admin-role-user --authDomain netbios-name --authPassword admin-user-password --truesso --list --authenticator
```

인증 옵션에 대한 자세한 내용은 [True SSO 구성을 위한 명령줄 참조](#)를 참조하십시오.

표 5-4. 인증자 관리를 위한 vdmutil truesso 명령 옵션

명령 및 옵션	설명
<code>--list --authenticator [--verbose]</code>	도메인에 있는 모든 SAML 인증자의 정규화된 도메인 이름(FQDN)을 나열합니다. 각각에 대해 True SSO의 사용 여부를 지정합니다. <code>--verbose</code> 옵션을 사용하는 경우는 연결된 연결 서버의 FQDN도 나열됩니다.
<code>--list --authenticator --name label</code>	지정된 인증자에 대해 True SSO의 사용 여부를 나열하고 연결된 연결 서버의 FQDN을 나열합니다. <code>--name</code> 옵션 없이 <code>--authenticator</code> 옵션을 사용할 때 나열되는 이름 중 하나를 <code>label</code> 로 사용합니다.
<code>--edit --authenticator --name label</code> <code>--truessoMode mode-value</code>	지정된 인증자에 대해 True SSO 모드를 지정한 값으로 설정하며, 여기서 <code>mode-value</code> 은 다음 값 중 하나일 수 있습니다. <ul style="list-style-type: none"> ■ ENABLED. 사용자의 Active Directory 자격 증명을 사용할 수 없는 경우에만 True SSO를 사용합니다. ■ ALWAYS. vIDM에 사용자의 AD 자격 증명 이 있더라도 항상 True SSO를 사용합니다. ■ DISABLED. True SSO를 사용하지 않도록 설정합니다. <code>--name</code> 옵션 없이 <code>--authenticator</code> 옵션을 사용할 때 <code>label</code> 에서는 나열된 이름 중 하나를 사용합니다.

True SSO에 대한 고급 구성 설정

Horizon Agent 시스템의 GPO 템플릿, 등록 서버의 레지스트리 설정, 연결 서버의 LDAP 항목을 사용하여 True SSO 고급 설정을 관리할 수 있습니다. 이러한 설정에는 기본 시간 초과, 로드 밸런싱 구성, 포함할 도메인 지정 등이 포함됩니다.

Horizon Agent 구성 설정

에이전트 OS에서 GPO 템플릿을 사용하여 풀 수준에서 True SSO를 끄거나 키 크기와 다시 연결 시도 수 및 설정과 같은 인증서 설정의 기본값을 변경할 수 있습니다.

참고 다음 표에는 개별 가상 시스템에서 에이전트를 구성하는 데 사용하는 설정이 나와 있지만 Horizon Agent 구성 템플릿 파일을 사용할 수도 있습니다. ADMX 템플릿 파일의 이름은 vdm_agent.admx입니다. 템플릿 파일을 사용하여 데스크톱 또는 애플리케이션 풀의 모든 가상 시스템에 이러한 정책 설정을 적용하도록 합니다. 설정된 정책은 레지스트리 설정보다 우선 순위가 높습니다.

ADMX 파일은 VMware 다운로드 사이트

<https://my.vmware.com/web/vmware/downloads>에서 사용할 수 있는 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip에 있습니다. Desktop & End-User Computing에서 ZIP 파일이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

표 5-5. Horizon Agent에 True SSO를 구성하기 위한 키

키	최소값 및 최 대값	설명
Disable True SSO	N/A	에이전트에서 기능을 사용하지 않도록 하려면 이 키를 true 로 설정합니다. 풀 수준에서 True SSO를 사용하지 않도록 하려면 그룹 정책에서 이 설정을 사용합니다. 기본값은 false 입니다.
Certificate wait timeout	10 -120	인증서가 에이전트에 도착할 때까지의 시간 초과 기간을 초 단위로 지정합니다. 기본값은 40 입니다.
Minimum key size	1024 - 8192	키에 대한 최소 허용 크기입니다. 기본값은 1024 이며, 이는 기본적으로 키 크기가 1024 미만이면 키를 사용할 수 없는 것을 의미합니다.
All key sizes	N/A	사용할 수 있는, 쉼표로 구분된 키 크기 목록입니다. 최대 5개의 크기를 지정할 수 있습니다(예: 1024,2048,3072,4096). 기본값은 2048 입니다.
Number of keys to pre-create	1-100	원격 데스크톱과 호스팅된 Windows 애플리케이션을 제공하는 RDS 서버에 미리 생성할 키의 수입니다. 기본값은 5 입니다.
Minimum validity period required for a certificate	N/A	사용자를 다시 연결하는 데 사용되는 인증서에 필요한 최소 유효 기간을 분 단위로 설정합니다. 기본값은 5 입니다.

등록 서버 구성 설정

등록 서버 OS에서 Windows 레지스트리 설정을 사용하여 연결할 도메인, 다양한 시간 초과 기간, 폴링 기간, 재시도, 같은 로컬 서버에 설치된 CA(인증 기관)를 선호하는지(권장)를 구성할 수 있습니다.

고급 구성 설정을 변경하려면 등록 서버 시스템에서 Windows 레지스트리 편집기(regedit.exe)를 열고 다음 레지스트리 키로 이동합니다.

```
HKLM\SOFTWARE\VMware, Inc.\VMware VDM\Enrollment Service
```

표 5-6. 등록 서버에 True SSO를 구성하기 위한 레지스트리 키

레지스트리 키	최소값 및 최 대값	유형	설명
ConnectToDomains	N/A	REG_MULTI_SZ	<p>등록 서버에서 자동으로 연결을 시도하는 도메인의 목록입니다. 이 다중 문자열 레지스트리 유형에 대해 각 도메인의 DNS FQDN(정규화된 도메인 이름)이 개별 행에 나열됩니다.</p> <p>기본으로 모든 도메인을 신뢰하도록 설정되어 있습니다.</p>
ExcludeDomains	N/A	REG_MULTI_SZ	<p>등록 서버에서 자동으로 연결하지 않는 도메인의 목록입니다. 연결 서버에서 도메인에 구성 설정을 제공할 경우에는 등록 서버에서 해당 도메인에 연결을 시도합니다. 이 다중 문자열 레지스트리 유형에 대해 각 도메인의 DNS FQDN이 개별 행에 나열됩니다.</p> <p>기본으로 도메인을 제외하지 않도록 설정되어 있습니다.</p>
ConnectToDomainsInForest	N/A	REG_SZ	<p>등록 서버가 속한 포리스트에서 모든 도메인에 연결하여 사용하는지를 지정합니다. 기본값은 TRUE입니다.</p> <p>다음 값 중 하나를 사용합니다.</p> <ul style="list-style-type: none"> ■ 0은 false를 의미합니다. 사용 중인 포리스트의 도메인에 연결하지 않습니다. ■ !=0은 true를 의미합니다.
ConnectToTrustingDomains	N/A	REG_SZ	<p>명시적으로 신뢰하는/수신하는 도메인에 연결하는지를 지정합니다. 기본값은 TRUE입니다.</p> <p>다음 값 중 하나를 사용합니다.</p> <ul style="list-style-type: none"> ■ 0은 false를 의미합니다. 명시적으로 신뢰하는/수신하는 도메인에 연결하지 않습니다. ■ !=0은 true를 의미합니다.
PreferLocalCa	N/A	REG_SZ	<p>로컬에 설치된 CA가 있는 경우 성능상의 이점을 위해 이 CA를 선호하는지 여부를 지정합니다. TRUE로 설정된 경우에는 등록 서버에서 로컬 CA로 요청을 보냅니다. 로컬 CA에 대한 연결이 실패하면 등록 서버에서 대체 CA로 인증서 요청을 보내려고 합니다. 기본값은 FALSE입니다.</p> <p>다음 값 중 하나를 사용합니다.</p> <ul style="list-style-type: none"> ■ 0은 false를 의미합니다. ■ !=0은 true를 의미합니다.
MaxSubmitRetryTime	9500 - 5900 0	DWORD	<p>인증서 서명 요청을 다시 제출하려고 시도하기 전에 기다리는 시간을 밀리초 단위로 지정합니다. 기본값은 25000입니다.</p>

표 5-6. 등록 서버에 True SSO를 구성하기 위한 레지스트리 키 (계속)

레지스트리 키	최소값 및 최 대값	유형	설명
SubmitLatencyWarningTime	500 - 5000	DWORD	<p>인터페이스에 '성능 저하' 표시가 되어 있는 경우에 지연 시간 경고 시간(밀리초 단위)을 제출합니다. 기본값은 1500입니다.</p> <p>등록 서버에서는 이 설정을 사용하여 CA를 성능 저하 상태로 간주해야 하는지를 결정합니다. 마지막 세 개의 인증서 요청을 완료하는 데 걸린 시간(밀리초)이 이 설정에 지정된 시간을 초과한 경우에는 해당 CA의 성능이 저하된 것으로 간주하며, 이 상태가 Horizon Administrator 상태 대시보드에 표시됩니다.</p> <p>CA에서는 일반적으로 20ms 이내에 인증서를 발급하지만, CA가 몇 시간 동안 유휴 상태였던 경우에는 초기 요청을 완료하는 데 시간이 더 오래 걸릴 수 있습니다. 이 설정을 사용하면 CA를 느린 것으로 표시하지 않아도 CA가 느릴 때 관리자가 이를 발견할 수 있습니다. 이 설정을 사용하여 CA를 느린 것으로 표시하기 위한 임계값을 구성합니다.</p>
WarnForLonglivedCert	N/A	REG_SZ	<p>수명이 긴 True SSO 인증서(템플릿)에 대한 경고를 사용하지 않도록 설정합니다. 기본값은 True입니다.</p> <p>등록 서버는 인증서 수명이 14일보다 길게 설정된 경우 True SSO 템플릿을 성능이 저하되었거나 최적 상태가 아닌 것으로 보고함으로써 Horizon Administrator 상태 대시보드에 경고 상태를 표시합니다. 등록 서버는 이 설정을 사용하여 경고를 사용하지 않도록 설정합니다.</p> <p>이 설정을 적용하려면 등록 서버를 다시 시작해야 합니다.</p>

연결 서버 구성 설정

연결 서버에서 View LDAP를 편집하여 인증서 생성 시간 초과와 등록 서버 사이에 인증서 요청 빨린싱을 사용하는지(권장) 여부를 구성할 수 있습니다.

고급 구성 설정을 변경하려면 연결 서버 호스트에서 ADSI 편집을 사용해야 합니다. 고유 이름 **DC=vdi**, **DC=vmware**, **DC=int**를 연결 지점으로 입력하고 컴퓨터의 서버 이름과 포트를 **localhost:389**로 입력하여 연결할 수 있습니다. **OU=Properties**를 확장한 다음 **OU=Global**을 선택하고 오른쪽 창에서 **CN=Common**을 두 번 클릭합니다.

그 후에 **pae-NameValuePair** 특성을 편집하여 다음 표에 나열된 값을 하나 이상 추가할 수 있습니다. 값을 추가할 때 이름 = 값 구문을 사용해야 합니다.

표 5-7. 연결 서버에 대한 고급 True SSO 설정

레지스트리 키	설명
cs-view-certss-enable-es-loadbalance=[true false]	두 개의 등록 서버 사이에서 로드 밸런싱 CSR 요청을 사용하는지 여부를 지정합니다. 기본값은 false입니다. 예를 들어, 로드 밸런싱을 사용하도록 설정하여 인증서 요청이 도착하면 연결 서버에서 대체 등록 서버를 사용하게 하려면 cs-view-certss-enable-es-loadbalance=true를 추가합니다. 등록 서버와 CA가 같은 호스트에 있는 경우에는 각 등록 서버에서 로컬 CA를 사용하여 요청을 서비스할 수 있습니다.
cs-view-certss-certgen-timeout-sec=숫자	CSR을 받은 후에 인증서를 생성할 때까지 기다리는 시간을 초 단위로 지정합니다. 기본값은 35입니다.

AD UPN이 없는 AD 사용자 식별

AD UPN이 없는 AD 사용자를 식별하도록 연결 서버에 대한 LDAP URL 필터를 구성할 수 있습니다.

연결 서버 호스트에서 ADAM ADSI 편집을 사용해야 합니다. 고유 이름 **DC=vdi**, **DC=vmware**, **DC=int**를 입력하여 연결할 수 있습니다. **OU=Properties**를 확장하고 **OU=Authenticator**를 선택합니다.

그런 후 **pae-LDAPURLList** 특성을 편집하여 LDAP URL 필터를 추가합니다.

예를 들어 다음 필터를 추가합니다.

```
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=ldap:///???(telephoneNumber=$NAMEID)
```

연결 서버는 다음 기본 LDAP URL 필터를 사용합니다.

```
urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified=ldap:///???(objectCategory=user)
(objectclass=user)(sAMAccountName=$NAMEID)) ldap:///???(objectCategory=group)
(objectclass=group)(sAMAccountName=$NAMEID))
```

```
urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified=ldap:///???(objectCategory=user)
(objectclass=user)(sAMAccountName=$NAMEID)) ldap:///???(objectCategory=group)
(objectclass=group)(sAMAccountName=$NAMEID))
```

LDAP URL 필터를 구성하는 경우 연결 서버는 사용자를 식별하는 데 이 LDAP URL 필터를 사용하며, 기본 LDAP URL 필터를 사용하지 않습니다.

AD UPN이 없는 AD 사용자의 SAML 인증에 사용할 수 있는 식별자 예:

- "cn"
- "mail"
- "description"
- "givenName"
- "sn"
- "canonicalName"

- "sAMAccountName"
- "member"
- "memberOf"
- "distinguishedName"
- "telephoneNumber"
- "primaryGroupID"

True SSO 및 Workspace ONE 을 사용하여 데스크톱 잠금 해제

True SSO를 사용하여 데스크톱에 로그인한 후에 동일한 로그인 자격 증명을 사용하여 Workspace ONE 포털에서 재인증한 후 데스크톱 잠금을 해제할 수 있습니다.

사전 요구 사항

- Horizon 7 버전 7.8 이상이 있는지 확인합니다.
- Windows용 Horizon Client 버전 5.0 이상이 있는지 확인합니다.
- VMware Identity Manager 버전 19.03 이상이 있는지 확인합니다.

절차

- 1 Workspace ONE을 사용하도록 설정하고 연결 서버와 함께 사용할 수 있도록 구성합니다.
[Workspace ONE 설명서](#) 웹 페이지에서 Workspace ONE 설명서를 참조하십시오.
- 2 True SSO에 대한 Horizon 연결 서버를 구성합니다.
[True SSO에 대한 Horizon 연결 서버 구성](#)의 내용을 참조하십시오.
- 3 가상 또는 게시된 데스크톱을 시작하려면 True SSO가 구성된 Workspace ONE 모드에서 연결 서버에 연결합니다. [VMware Horizon Client 설명서](#) 웹 페이지에서 Horizon Client 설명서를 참조하십시오.
- 4 사용자가 True SSO에서 Single Sign-On을 사용할 수 있도록 Workspace ONE 포털에서 가상 또는 게시된 데스크톱을 시작합니다.
- 5 데스크톱을 잠급니다.
- 6 데스크톱의 잠금을 해제하려면 **VMware True SSO 사용자**를 선택하고 **제출**을 클릭합니다.

다음에 수행할 작업

Horizon Agent가 설치된 시스템의 다음 위치에서 레지스트리 키를 설정하여 이 기능을 사용하지 않도록 설정할 수 있습니다.

```
HKLM\Software\VMware, Inc.\VMware VDM\Agent\WCertSSO[DisableCertSSOUnlock=true]
```


다음 위치에서 Windows용 Horizon Client의 레지스트리 키 DisabledFeatures=TrueSSOLock을 설정하여 이 기능을 사용하지 않도록 설정할 수도 있습니다.

- Windows 32비트 운영 체제: [HKEY_CURRENT_USER\Software\VMware, Inc.\VMware VDMWClient] 또는 [HKEY_LOCAL_MACHINE\Software\VMware, Inc.\VMware VDMWClient].
- Windows 64비트 운영 체제: [HKEY_CURRENT_USER\Software\Wow6432Node\VMware, Inc.\VMware VDMWClient] 또는 [HKEY_LOCAL_MACHINE\Software\Wow6432Node\VMware, Inc.\VMware VDMWClient].

이 레지스트리 키를 설정하면 사용자가 데스크톱의 잠금을 해제할 때 **VMware True SSO 사용자** 옵션이 표시되지 않습니다.

시스템 상태 대시보드를 사용하여 True SSO와 관련된 문제 해결

Horizon Administrator에서 시스템 상태 대시보드를 사용하여 True SSO 기능의 작동에 영향을 줄 수 있는 문제를 빠르게 확인할 수 있습니다.

최종 사용자의 경우 True SSO가 작동을 중지하면 시스템에서 사용자가 원격 데스크톱이나 애플리케이션에 로그인하려고 할 때 "사용자 이름 또는 암호가 정확하지 않습니다."라는 메시지가 사용자에게 표시됩니다. 사용자가 **확인**을 클릭하면 로그인 화면으로 이동합니다. Windows 로그인 화면에서 사용자에게 **VMware SSO 사용자**라는 레이블이 있는 추가 타일이 표시됩니다. 권한이 부여된 사용자를 위한 Active Directory 자격 증명이 사용자에게 있는 경우에는 AD 자격 증명으로 로그인할 수 있습니다.

Horizon Administrator 디스플레이의 왼쪽 위에 있는 시스템 상태 대시보드에는 True SSO와 관련된 항목 두 개가 있습니다.

참고 True SSO 기능은 1분에 한 번만 대시보드에 정보를 제공합니다. 정보를 즉시 새로 고치려면 오른쪽 상단에 있는 새로 고침 아이콘을 클릭하십시오.

- **View 구성 요소 > True SSO**를 클릭하여 확장하면 True SSO를 사용하는 도메인의 목록을 볼 수 있습니다.

도메인 이름을 클릭하면 해당 도메인에 구성된 등록 서버의 목록, 회사 CA(인증 기관)의 목록, 사용 중인 인증서 템플릿의 이름, 상태 정보를 볼 수 있습니다. 문제가 있을 경우에는 상태 필드에 설명이 표시됩니다.

True SSO 도메인 세부 정보 대화상자에 표시되는 구성 설정을 변경하려면 vdmutil 명령줄 인터페이스를 사용하여 True SSO 커넥터를 편집합니다. 자세한 내용은 [커넥터 관리 명령](#)의 내용을 참조하십시오.

- **기타 구성 요소 > SAML 2.0 인증자**를 클릭하여 확장하면 VMware Identity Manager 인스턴스에 인증을 위임하기 위해 생성된 SAML 인증자의 목록을 볼 수 있습니다. 인증자 이름을 클릭하면 세부 정보와 상태를 확인할 수 있습니다.

참고 True SSO를 사용하려면 SSO의 전역 설정을 사용하도록 설정해야 합니다. Horizon Administrator에서 **구성 > 전역 설정**을 선택하고 **SSO(Single Sign-On)**가 **사용**으로 설정되어 있는지 확인합니다.

표 5-8. 연결 서버-등록 서버 간 연결 상태

상태 텍스트	설명
True SSO 상태 정보를 가져오지 못했습니다.	대시보드가 연결 서버 인스턴스에서 상태 정보를 검색할 수 없습니다.
True SSO 구성 서비스에서 <FQDN> 등록 서버에 연결할 수 없습니다.	포드에서 연결 서버 인스턴스 중 하나가 포드가 사용하는 모든 등록 서버에 구성 정보를 보내도록 선택되었습니다. 이 연결 서버 인스턴스는 1분 간격으로 등록 서버 구성을 새로 고칩니다. 구성 작업에서 등록 서버 업데이트에 실패할 경우 이 메시지가 표시됩니다. 자세한 내용은 등록 서버 연결 표를 참조하십시오.
이 연결 서버에서 세션을 관리하기 위해 <FQDN> 등록 서버에 접속할 수 없습니다.	현재 연결 서버 인스턴스에서 등록 서버에 연결할 수 없습니다. 이 상태는 브라우저에서 가리키는 연결 서버 인스턴스에 대해서만 표시됩니다. 포드에 연결 서버 인스턴스가 여러 개 있는 경우에는 브라우저에서 상태 확인을 위해 다른 연결 서버 인스턴스를 가리키도록 변경해야 합니다. 자세한 내용은 등록 서버 연결 표를 참조하십시오.

표 5-9. 등록 서버 연결

상태 텍스트	설명
이 도메인 <Domain Name>이 (가) <FQDN> 등록 서버에 없습니다.	True SSO 커넥터가 해당 도메인에 이 등록 서버를 사용하도록 구성되었지만, 아직 등록 서버가 이 도메인에 연결하도록 구성되지 않았습니다. 상태가 1분 넘게 계속되는 경우에는 현재 등록 구성 새로 고침을 담당하는 연결 서버 인스턴스의 상태를 확인해야 합니다.
<FQDN> 등록 서버에서 아직 도메인 <Domain Name>에 연결하는 중입니다.	등록 서버에서 이 도메인의 도메인 컨트롤러에 연결하지 못했습니다. 이 상태가 1분 넘게 계속되는 경우에는 등록 서버에서 도메인으로의 이름 확인이 올바른지 확인하고 등록 서버와 도메인 간에 네트워크가 연결되어 있는지 확인해야 합니다.
<FQDN> 등록 서버에서 도메인 <Domain Name>(으)로의 연결이 중지되고 있거나 문제가 발생한 상태입니다.	등록 서버가 도메인의 도메인 컨트롤러에 연결되었지만 도메인 컨트롤러에서 PKI 정보를 읽지 못했습니다. 이 경우는 실제 도메인 컨트롤러에 문제가 있을 가능성이 큼니다. DNS가 올바르게 구성되지 않은 경우에도 이 문제가 발생할 수 있습니다. 등록 서버의 로그 파일을 확인하여 등록 서버에서 사용하려는 도메인 컨트롤러가 무엇이며 도메인 컨트롤러가 올바르게 작동하고 있는지 확인하십시오.
<FQDN> 등록 서버가 아직 도메인 컨트롤러에서 등록 속성을 읽지 않았습니다.	이 상태는 일시적이며 등록 서버를 시작하는 동안이나 새 도메인이 환경에 추가된 경우에만 표시됩니다. 이 상태는 일반적으로 지속 시간이 1분 미만입니다. 이 상태가 1분 넘게 계속되는 경우에는 네트워크가 심하게 느리거나 도메인 컨트롤러 액세스를 방해하는 문제가 발생한 것입니다.
<FQDN> 등록 서버에서 등록 속성을 한 번 이상 읽었지만 일시적으로 도메인 컨트롤러에 연결하지 못했습니다.	등록 서버가 도메인 컨트롤러에서 PKI 구성을 읽는 동안에는 2분 간격으로 변경 사항을 폴링합니다. DC(도메인 컨트롤러)에 일시적으로 연결하지 못한 경우 이 상태가 설정됩니다. 이렇게 DC에 연결할 수 없을 경우 일반적으로 등록 서버에서 PKI 구성의 변경 사항을 감지하지 못하는 것일 수 있습니다. 인증서 서버에서 도메인 컨트롤러에 액세스할 수 있는 한, 인증서는 계속 발급할 수 있습니다.
<FQDN> 등록 서버에서 등록 속성을 한 번 이상 읽었지만 오랫동안 도메인 컨트롤러에 연결하지 못했거나 다른 문제가 있습니다.	등록 서버에서 오랫동안 도메인 컨트롤러에 연결하지 못한 경우에 이 상태가 표시됩니다. 그런 다음 등록 서버에서 이 도메인의 대체 도메인 컨트롤러를 찾으려고 합니다. 인증서 서버에서 도메인 컨트롤러에 액세스할 수 있으면 인증서를 발급할 수 있지만, 이 상태가 1분 넘게 계속될 경우 등록 서버에서 도메인의 모든 도메인 컨트롤러에 액세스하지 못함을 의미하며 더 이상 인증서를 발급할 수 없을 가능성이 큼니다.

표 5-10. 등록 인증서 상태

상태 텍스트	설명
이 도메인의 <domain name> 포리스트에 유효한 등록 인증서가 <FQDN> 등록 서버에 설치되지 않았거나 만료되었을 수 있습니다.	이 도메인에 대한 등록 인증서가 설치되지 않았거나, 인증서가 유효하지 않거나 만료되었습니다. 등록 인증서는 이 도메인이 속한 포리스트가 신뢰하는 회사 CA에서 발급한 것이어야 합니다. 등록 서버에 등록 인증서를 설치하는 방법이 설명된 Horizon 7 관리 문서의 단계를 완료했는지 확인하십시오. 인증서 관리 스냅인인 MMC를 열어 로컬 컴퓨터 저장소를 열 수도 있습니다. 개인 인증서 컨테이너를 열고 인증서가 설치되어 있으며 유효한지 확인하십시오. 등록 서버 로그 파일을 열 수도 있습니다. 등록 서버에는 저장되어 있는 인증서의 상태에 대한 추가 정보가 기록됩니다.

표 5-11. 인증서 템플릿 상태

상태 텍스트	설명
템플릿 <name>이(가) <FQDN> 등록 서버 도메인에 없습니다.	올바른 템플릿 이름을 지정했는지 확인하십시오.
이 템플릿에서 생성된 인증서는 Windows 로그인에 사용할 수 없습니다.	이 템플릿은 스마트 카드와 데이터 서명을 사용하도록 설정되지 않았습니다. 올바른 템플릿 이름을 지정했는지 확인하십시오. True SSO에 사용하는 인증서 템플릿 만들기 에 설명된 단계를 완료했는지 확인하십시오.
템플릿 <name>에서 스마트 카드 로그인을 사용하도록 설정되어 있지만 사용할 수 없습니다.	이 템플릿에서 스마트 카드 로그인을 사용하도록 설정되어 있지만 True SSO에 템플릿을 사용할 수 없습니다. 올바른 템플릿 이름을 지정했는지 확인하고 True SSO에 사용하는 인증서 템플릿 만들기 에 설명된 단계를 완료했는지 확인하십시오. 템플릿에서 True SSO를 사용하지 못하게 하는 설정이 무엇이라고 기록되었는지 알아보기 위해 등록 서버 로그 파일을 확인할 수도 있습니다.

표 5-12. 인증서 서버 구성 상태

상태 텍스트	설명
인증서 서버 <CN of CA>이(가) 도메인에 없습니다.	CA에 올바른 이름을 지정했는지 확인하십시오. CN(일반 이름)을 지정해야 합니다.
인증서가 NTAUTH(Enterprise) 저장소에 없습니다.	이 CA가 회사 CA가 아니거나 CA 인증서가 NTAUTH 저장소에 추가되지 않았습니다. 이 CA가 포리스트의 구성원이 아닌 경우에는 CA 인증서를 이 포리스트의 NTAUTH 저장소에 수동으로 추가해야 합니다.

표 5-13. 인증서 서버 연결 상태

상태 텍스트	설명
<FQDN> 등록 서버가 인증서 서버 <CN of CA>에 연결되지 않았습니다.	등록 서버가 인증서 서버에 연결되지 않았습니다. 등록 서버가 방금 시작되었거나 CA가 True SSO 커넥터에 최근에 추가된 경우에는 이 상태가 일시적인 것일 수 있습니다. 상태가 1분 넘게 계속되는 경우에는 등록 서버에서 CA에 연결하지 못한 것입니다. 이름 확인이 올바르게 작동하고, CA에 네트워크가 연결되어 있으며, 등록 서버의 시스템 계정에 CA에 액세스할 권한이 있는지 확인하십시오.
<FQDN> 등록 서버가 인증서 서버 <CN of CA>에 연결되었지만 인증서 서버의 성능이 저하된 상태에 있습니다.	CA의 인증서 발급이 느린 경우에 이 상태가 표시될 수 있습니다. CA가 이 상태로 남아 있는 경우에는 CA나 CA에서 사용하는 도메인 컨트롤러의 로드를 확인하십시오. 참고 CA가 느린 것으로 표시된 경우에는 인증서 요청을 하나 이상 완료하고, 정상적인 기간 안에 인증서가 발급될 때까지 이 상태를 유지합니다.
<FQDN> 등록 서버가 인증서 서버 <CN of CA>에 연결할 수 있지만 서비스를 사용할 수 없습니다.	등록 서버에 CA에 대한 활성 연결이 있지만 인증서를 발급할 수 없는 경우에 이 상태가 표시됩니다. 이 상태는 일반적으로 일시적인 상태입니다. CA를 즉시 사용할 수 없는 경우에는 상태가 연결 해제로 변경됩니다.

역할 기반 위임된 관리 구성

Horizon 7 환경에서 한 가지 주요 관리 작업은 Horizon Administrator를 이용할 수 있는 사용자와 이들이 수행할 수 있도록 권한을 부여할 작업을 결정하는 것입니다. 역할 기반 위임된 관리를 사용해 특정 Active Directory 사용자 및 그룹에 관리자 역할을 할당함으로써 관리 역할을 선택하여 할당할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 역할 및 권한 이해
- 액세스 그룹을 사용하여 풀 및 팜 관리 위임
- 사용 권한 이해
- 관리자 관리
- 사용 권한 관리 및 검토
- 액세스 그룹 관리 및 검토
- 사용자 지정 역할 관리
- 미리 정의된 역할 및 권한
- 일반 작업에 필요한 권한
- 관리자 사용자 및 그룹의 모범 사례

역할 및 권한 이해

Horizon Administrator에서 작업 수행 기능은 관리자 역할과 권한으로 구성되는 액세스 제어 시스템에서 관리합니다. 이 시스템은 vCenter Server 액세스 컨트롤 시스템과 유사합니다.

관리자 역할은 권한의 집합입니다. 권한은 사용자에게 데스크톱 풀에 대한 권한 부여와 같은 특정 작업을 수행할 수 있는 능력을 부여합니다. 또한 권한은 관리자가 Horizon Administrator에서 볼 수 있는 내용을 제어합니다. 예를 들어, 관리자에게 전역 정책을 보거나 수정할 수 있는 권한이 없는 경우, 관리자가 Horizon Administrator에 로그인할 때 **전역 정책** 설정이 탐색 패널에 표시되지 않습니다.

관리자 권한은 전역 또는 개체 특정입니다. 전역 권한을 가지고 있으면 전역 설정 보기 및 변경 등과 같은 시스템 차원의 작업을 제어할 수 있습니다. 개체 특정 권한은 특정 유형의 개체에 대한 작업을 제어합니다.

관리자 역할은 일반적으로 높은 수준의 관리 작업을 수행하는 데 필요한 모든 개별 권한을 조합합니다. Horizon Administrator에는 일반적인 관리 작업을 수행하는 데 필요한 권한을 포함하는 미리 정의된 역할이 포함됩니다. 이러한 미리 정의된 역할을 관리자 사용자 및 그룹에 할당하거나 선택한 권한을 조합하여 고유 역할을 생성할 수 있습니다. 미리 정의된 역할을 수정할 수 없습니다.

관리자를 생성하려면 Active Directory 사용자 및 그룹에서 사용자 및 그룹을 선택하고 관리자 역할을 할당합니다. 관리자는 역할 할당을 통해 권한을 얻습니다. 관리자에 직접 권한을 할당할 수 없습니다. 여러 역할 할당을 가진 관리자는 해당 역할에 포함된 모든 권한 전체를 얻습니다.

액세스 그룹을 사용하여 폴 및 팜 관리 위임

기본적으로 자동화된 데스크톱 폴, 수동 데스크톱 및 팜이 루트 액세스 그룹에 생성되며 Horizon Administrator에 / 또는 루트(/)로 나타납니다. 게시된 데스크톱 폴 및 애플리케이션 폴은 해당 팜의 액세스 그룹을 상속합니다. 루트 액세스 그룹 아래에 액세스 그룹을 생성하여 다른 관리자에게 특정 폴 또는 팜 관리를 위임할 수 있습니다.

참고 게시된 데스크톱 폴 또는 애플리케이션 폴의 액세스 그룹은 직접 변경할 수 없습니다. 게시된 데스크톱 폴 또는 애플리케이션 폴이 속한 팜의 액세스 그룹을 변경해야 합니다.

가상 또는 물리적 시스템은 해당 데스크톱 폴의 액세스 그룹을 상속합니다. 연결된 영구 디스크는 해당 시스템의 액세스 그룹을 상속합니다. 루트 액세스 그룹을 포함하여 최대 100개의 액세스 그룹을 가질 수 있습니다.

관리자에게 해당 액세스 그룹에 대한 역할을 할당하여 액세스 그룹의 리소스에 대한 관리자 액세스를 구성합니다. 관리자는 역할을 할당받은 액세스 그룹에만 있는 리소스에 액세스할 수 있습니다. 관리자가 액세스 그룹에 대해 가진 역할에 따라 해당 액세스 그룹의 리소스에 대한 관리자 액세스 수준이 결정됩니다.

루트 액세스 그룹의 역할이 상속되기 때문에 루트 액세스 그룹에 대한 역할을 가진 관리자는 모든 액세스 그룹에 대해 해당 역할을 가집니다. 루트 액세스 그룹에 대한 관리자 역할을 가진 관리자는 시스템의 모든 개체에 대해 전체 액세스 권한을 가지기 때문에 슈퍼 관리자입니다.

역할에는 액세스 그룹에 적용할 개체 특정 권한이 하나 이상 있어야 합니다. 전역 권한만 포함된 역할은 액세스 그룹에 적용할 수 없습니다.

Horizon Administrator를 사용하여 액세스 그룹을 생성하고 기존 데스크톱 폴을 액세스 그룹으로 이동할 수 있습니다. 자동화된 데스크톱 폴, 수동 폴 또는 팜을 생성할 경우 기본 루트 액세스 그룹을 그대로 사용하거나 다른 액세스 그룹을 선택할 수 있습니다.

참고 VMware Identity Manager를 통해 데스크톱 및 애플리케이션에 대한 액세스를 제공하려는 경우 Horizon Administrator에서 루트 액세스 그룹에 대한 관리자 역할을 가진 사용자로 데스크톱 및 애플리케이션 폴을 생성하는지 확인해야 합니다. 사용자에게 루트 액세스 그룹이 아닌 다른 액세스 그룹에 대한 관리자 역할을 부여할 경우 VMware Identity Manager가 Horizon 7에 구성된 SAML 인증자를 인식하지 못하므로 VMware Identity Manager에 폴을 구성할 수 없습니다.

■ 다른 액세스 그룹에 다른 관리자 생성

서로 다른 관리자를 생성해 구성 내의 각 액세스 그룹을 관리할 수 있습니다.

■ 같은 액세스 그룹에 다른 관리자 생성

서로 다른 관리자를 생성해 같은 액세스 그룹을 관리하도록 할 수 있습니다.

다른 액세스 그룹에 다른 관리자 생성

서로 다른 관리자를 생성해 구성 내의 각 액세스 그룹을 관리할 수 있습니다.

예를 들어, 한 액세스 그룹에는 회사 데스크톱 풀이 있고, 다른 액세스 그룹에는 소프트웨어 개발자용 데스크톱 풀이 있으면 서로 다른 관리자를 생성해 각 액세스 그룹의 리소스를 관리할 수 있습니다.

표6-1에서는 이러한 구성 유형의 예제를 보여줍니다.

표 6-1. 다른 액세스 그룹에 다른 관리자 생성

관리자	역할	액세스 그룹
view-domain.com\Admin1	인벤토리 관리자	/CorporateDesktops
view-domain.com\Admin2	인벤토리 관리자	/DeveloperDesktops

이 예제에서 관리자 Admin1은 CorporateDesktops 액세스 그룹에 대해 인벤토리 관리자 역할을 가지고 있고 관리자 Admin2는 DeveloperDesktops 액세스 그룹에 대해 인벤토리 관리자 역할을 가지고 있습니다.

같은 액세스 그룹에 다른 관리자 생성

서로 다른 관리자를 생성해 같은 액세스 그룹을 관리하도록 할 수 있습니다.

예를 들어, 여러 기업 데스크톱 풀이 하나의 액세스 그룹에 있으면 이들 풀을 확인하고 수정할 수 있는 관리자 한 명과 확인만 할 수 있는 관리자 한 명을 따로 생성할 수 있습니다.

표6-2에서는 이러한 구성 유형의 예제를 보여줍니다.

표 6-2. 같은 액세스 그룹에 다른 관리자 생성

관리자	역할	액세스 그룹
view-domain.com\Admin1	인벤토리 관리자	/CorporateDesktops
view-domain.com\Admin2	인벤토리 관리자(읽기 전용)	/CorporateDesktops

이 예제에서 관리자 Admin1은 CorporateDesktops 액세스 그룹에 대해 인벤토리 관리자 역할을 가지고 있고 관리자 Admin2는 같은 액세스 그룹에 대해 인벤토리 관리자(읽기 전용) 역할을 가지고 있습니다.

사용 권한 이해

Horizon Administrator는 역할, 관리자 사용자 또는 그룹 및 액세스 그룹의 조합을 사용 권한으로 나타냅니다. 역할은 수행할 수 있는 작업을 정의하고 사용자 또는 그룹은 작업을 수행할 수 있는 사용자를 나타내며, 액세스 그룹은 작업의 대상이 되는 개체를 포함합니다.

사용 권한은 관리자 사용자나 그룹, 액세스 그룹 또는 역할을 선택했는지에 따라 Horizon Administrator에 다르게 나타납니다.

다음 표에는 관리자 사용자 또는 그룹을 선택할 때 사용 권한이 Horizon Administrator에 어떻게 나타나는지 나와 있습니다. 관리자 사용자는 Admin 1로 불리며 두 가지 사용 권한을 갖고 있습니다.

표 6-3. Admin 1의 관리자 및 그룹 탭 사용 권한

역할	액세스 그룹
인벤토리 관리자	MarketingDesktops
관리자(읽기 전용)	/

첫 번째 사용 권한은 Admin 1에 MarketingDesktops라는 액세스 그룹에 대한 인벤토리 관리자 역할이 있음을 보여 줍니다. 두 번째 사용 권한은 Admin 1에 루트 액세스 그룹에 대한 관리자(읽기 전용) 역할이 있음을 보여 줍니다.

다음 표에는 MarketingDesktops 액세스 그룹을 선택할 경우 동일한 사용 권한이 Horizon Administrator에 어떻게 표시되는지 나와 있습니다.

표 6-4. MarketingDesktops의 폴더 탭 사용 권한

Admin	역할	상속됨
view-domain.com\Admin1	인벤토리 관리자	
view-domain.com\Admin1	관리자(읽기 전용)	예

첫 번째 사용 권한은 표 6-3에 표시된 첫 번째 사용 권한과 동일합니다. 두 번째 사용 권한은 표 6-3에 표시된 두 번째 사용 권한에서 상속됩니다. 액세스 그룹은 루트 액세스 그룹의 사용 권한을 상속하기 때문에 Admin1은 MarketingDesktops 액세스 그룹에서 관리자(읽기 전용) 역할을 갖습니다. 사용 권한이 상속된 경우 상속됨 열에 예가 나타납니다.

다음 표에는 인벤토리 관리자 역할을 선택할 때 표 6-3의 첫 번째 사용 권한이 Horizon Administrator에서 어떻게 나타나는지 나와 있습니다.

표 6-5. 인벤토리 관리자의 역할 탭 사용 권한

Administrator	액세스 그룹
view-domain.com\Admin1	/MarketingDesktops

관리자 관리

관리자 역할을 가진 사용자는 Horizon Administrator를 사용해 관리자 사용자 및 그룹을 추가 및 제거할 수 있습니다.

관리자 역할은 Horizon Administrator에서 가장 강력한 역할입니다. 처음에는 Administrators 계정의 구성원에 관리자 역할이 부여됩니다. 연결 서버를 설치할 때 Administrators 계정을 지정합니다. Administrator 계정은 연결 서버 컴퓨터 또는 도메인 사용자 또는 그룹 계정의 로컬 관리자 그룹(BUILTIN\Administrators)이 될 수 있습니다.

참고 기본적으로 도메인 관리자 그룹은 로컬 관리자 그룹 구성원입니다. Administrators 계정을 로컬 Administrators 그룹으로 지정했으며, 도메인 관리자에게 인벤토리 개체 및 Horizon 7 구성 설정에 대한 모든 액세스 권한을 부여하지 않으려는 경우, 로컬 관리자 그룹에서 도메인 관리자 그룹을 제거해야 합니다.

■ 관리자 생성

관리자를 생성하려면 Horizon Administrator의 Active Directory 사용자 및 그룹에서 사용자 또는 그룹을 선택하고 관리자 역할을 할당하십시오.

■ 관리자 제거

관리자 사용자 또는 그룹을 제거할 수 있습니다. 시스템의 마지막 슈퍼 관리자는 제거할 수 없습니다. 슈퍼 관리자는 루트 액세스 그룹에 대해 관리자 역할을 가진 관리자입니다.

관리자 생성

관리자를 생성하려면 Horizon Administrator의 Active Directory 사용자 및 그룹에서 사용자 또는 그룹을 선택하고 관리자 역할을 할당하십시오.

사전 요구 사항

- 미리 정의된 관리자 역할을 숙지합니다. [미리 정의된 역할 및 권한](#)을 참조하십시오.
- 관리자 사용자 및 그룹을 생성하는 모범 사례를 숙지합니다. [관리자 사용자 및 그룹의 모범 사례](#)를 참조하십시오.
- 관리자에 사용자 지정 역할을 할당하려면 사용자 지정 역할을 생성하십시오. [사용자 지정 역할 추가](#)를 참조하십시오.
- 특정 데스크톱 풀을 관리할 수 있는 관리자를 생성하려면 액세스 그룹을 생성한 후 데스크톱 풀을 해당 액세스 그룹으로 이동합니다. [액세스 그룹 관리 및 검토](#)를 참조하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 관리자**를 선택합니다.
- 2 **관리자 및 그룹** 탭에서 **사용자 또는 그룹 추가**를 클릭합니다.
- 3 검색 조건에 따라 Active Directory 사용자 또는 그룹을 필터링하려면 **추가**를 클릭하고 검색 조건을 하나 이상 선택한 다음 **찾기**를 클릭합니다.
- 4 관리자 사용자 또는 그룹으로 지정할 Active Directory 사용자 또는 그룹을 선택하고 **확인**을 클릭한 다음 **다음**을 클릭합니다.

Ctrl와 Shift 키를 눌러 사용자와 그룹을 여러 개 선택할 수 있습니다.

- 5 관리자 사용자 또는 그룹에 할당할 역할을 선택합니다.

액세스 그룹에 적용 열은 역할이 액세스 그룹에 적용되는지 여부를 나타냅니다. 개체별 권한이 포함된 역할만 액세스 그룹에 적용되며, 전역 권한만 포함된 역할은 액세스 그룹에 적용되지 않습니다.

옵션	조치
액세스 그룹에 선택한 역할 적용	액세스 그룹을 하나 이상 선택하고 다음 을 클릭합니다.
모든 액세스 그룹에 역할 적용	루트 액세스 그룹을 선택하고 다음 을 클릭합니다.

- 6 관리자 사용자 또는 그룹을 생성하려면 **마침**을 클릭합니다.

관리자 및 그룹 탭의 왼쪽 창에 새 관리자 사용자 또는 그룹이 표시되고, 선택한 역할과 액세스 그룹이 오른쪽 창에 표시됩니다.

관리자 제거

관리자 사용자 또는 그룹을 제거할 수 있습니다. 시스템의 마지막 수퍼 관리자는 제거할 수 없습니다. 수퍼 관리자는 루트 액세스 그룹에 대해 관리자 역할을 가진 관리자입니다.

절차

- 1 View Administrator에서 **View 구성 > 관리자**를 선택합니다.
- 2 **관리자 및 그룹** 탭에서 관리자 사용자 또는 그룹을 선택하고 **사용자 또는 그룹 제거**를 클릭하고 **확인**을 클릭합니다.

관리자 사용자 또는 그룹이 **관리자 및 그룹** 탭에 더 이상 나타나지 않습니다.

사용 권한 관리 및 검토

Horizon Administrator를 사용하여 특정 관리자 사용자와 그룹, 특정 역할 및 특정 액세스 그룹에 대한 사용 권한을 추가, 삭제 및 검토할 수 있습니다.

■ 사용 권한 추가

특정 관리자 사용자나 그룹, 특정 역할 또는 특정 액세스 그룹을 포함하는 사용 권한을 추가할 수 있습니다.

■ 사용 권한 삭제

특정 관리자 사용자 또는 그룹, 특정 역할 또는 특정 액세스 그룹을 포함하는 권한을 삭제할 수 있습니다.

■ 사용 권한 검토

특정 관리자나 그룹, 특정 역할 또는 특정 액세스 그룹을 포함하는 사용 권한을 검토할 수 있습니다.

사용 권한 추가

특정 관리자 사용자나 그룹, 특정 역할 또는 특정 액세스 그룹을 포함하는 사용 권한을 추가할 수 있습니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 관리자**를 선택합니다.

2 사용 권한을 생성하십시오.

옵션	조치
특정 관리자 사용자 또는 그룹을 포함하는 사용 권한 생성	<ul style="list-style-type: none"> a 관리자 및 그룹 탭에서 관리자 또는 그룹을 선택하고 사용 권한 추가를 클릭합니다. b 역할을 선택합니다. c 해당 역할이 액세스 그룹에 적용되지 않을 경우 마침을 클릭합니다. d 해당 역할이 액세스 그룹에 적용될 경우 다음을 클릭하고 액세스 그룹을 하나 이상 선택한 다음 마침을 클릭합니다. 역할에는 액세스 그룹에 적용할 개체 특정 권한이 하나 이상 있어야 합니다.
특정 역할을 포함하는 사용 권한 생성	<ul style="list-style-type: none"> a 역할 탭에서 역할을 선택하고 사용 권한을 클릭한 다음 사용 권한 추가를 클릭합니다. b 검색 조건에 맞는 관리자 사용자 또는 그룹을 찾으려면 추가를 클릭하고 검색 조건을 하나 이상 선택한 다음 찾기를 클릭합니다. c 사용 권한에 포함시킬 관리자 사용자 또는 그룹을 선택하고 확인을 클릭합니다. Ctrl와 Shift 키를 눌러 사용자와 그룹을 여러 개 선택할 수 있습니다. d 해당 역할이 액세스 그룹에 적용되지 않을 경우 마침을 클릭합니다. e 해당 역할이 액세스 그룹에 적용될 경우 다음을 클릭하고 액세스 그룹을 하나 이상 선택한 다음 마침을 클릭합니다. 역할에는 액세스 그룹에 적용할 개체 특정 권한이 하나 이상 있어야 합니다.
특정 액세스 그룹을 포함하는 사용 권한 생성	<ul style="list-style-type: none"> a 액세스 그룹 탭에서 액세스 그룹을 선택하고 사용 권한 추가를 클릭합니다. b 검색 조건에 맞는 관리자 사용자 또는 그룹을 찾으려면 추가를 클릭하고 검색 조건을 하나 이상 선택한 다음 찾기를 클릭합니다. c 사용 권한에 포함시킬 관리자 사용자 또는 그룹을 선택하고 확인을 클릭합니다. Ctrl와 Shift 키를 눌러 사용자와 그룹을 여러 개 선택할 수 있습니다. d 다음을 클릭하고 역할을 선택한 다음 마침을 클릭합니다. 역할에는 액세스 그룹에 적용할 개체 특정 권한이 하나 이상 있어야 합니다.

사용 권한 삭제

특정 관리자 사용자 또는 그룹, 특정 역할 또는 특정 액세스 그룹을 포함하는 권한을 삭제할 수 있습니다.

관리자 사용자 또는 그룹의 마지막 사용 권한을 제거하면 해당 관리자 사용자 또는 그룹도 제거됩니다. 루트 액세스 그룹에서 관리자 역할을 가진 관리자가 최소 한 명은 있어야 하기 때문에 해당 관리자를 제거하는 권한은 제거할 수 없습니다. 상속된 사용 권한을 삭제할 수 없습니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 관리자**를 선택합니다.

2 삭제할 사용 권한을 선택합니다.

옵션	조치
특정 관리자 또는 그룹에 적용되는 사용 권한을 삭제하십시오.	관리자 및 그룹 탭에서 관리자 또는 그룹을 선택합니다.
특정 역할에 적용되는 사용 권한을 삭제하십시오.	역할 탭에서 역할을 선택합니다.
특정 액세스 그룹에 적용되는 권한 삭제	액세스 그룹 탭에서 폴더를 선택합니다.

3 사용 권한을 선택하고 **사용 권한 삭제**를 클릭합니다.

사용 권한 검토

특정 관리자나 그룹, 특정 역할 또는 특정 액세스 그룹을 포함하는 사용 권한을 검토할 수 있습니다.

절차

- 1 **View 구성 > 관리자**를 선택합니다.
- 2 사용 권한을 검토하십시오.

옵션	조치
특정 관리자 또는 그룹을 포함하는 사용 권한 검토	관리자 및 그룹 탭에서 관리자 또는 그룹을 선택합니다.
특정 역할을 포함하는 사용 권한 검토	역할 탭에서 역할을 선택하고 사용 권한 을 클릭합니다.
특정 액세스 그룹을 포함하는 사용 권한 검토	액세스 그룹 탭에서 폴더를 선택합니다.

액세스 그룹 관리 및 검토

Horizon Administrator를 사용해 액세스 그룹을 추가 및 삭제하고 특정 액세스 그룹에 있는 데스크톱 풀과 시스템을 검토할 수 있습니다.

■ 액세스 그룹 추가

액세스 그룹을 생성하여 다른 관리자에게 특정 시스템, 데스크톱 풀 또는 팜 관리를 위임할 수 있습니다. 기본적으로 데스크톱 풀, 애플리케이션 풀 및 팜은 루트 액세스 그룹에 상주합니다.

■ 다른 액세스 그룹으로 데스크톱 풀 또는 팜 이동

액세스 그룹을 생성한 후 자동화된 데스크톱 풀, 수동 풀 또는 팜을 새 액세스 그룹으로 이동할 수 있습니다.

■ 액세스 그룹 제거

개체가 포함되지 않은 액세스 그룹을 제거할 수 있습니다. 루트 액세스 그룹은 제거할 수 없습니다.

■ 액세스 그룹의 데스크톱 풀, 애플리케이션 풀 또는 팜 검토

Horizon Administrator에서는 특정 액세스 그룹의 데스크톱 풀, 애플리케이션 풀 또는 팜을 볼 수 있습니다.

■ 액세스 그룹의 vCenter 가상 시스템 검토

Horizon Administrator에서 특정 액세스 그룹의 vCenter 가상 시스템을 검토할 수 있습니다. vCenter 가상 시스템은 해당 풀의 액세스 그룹을 상속합니다.

액세스 그룹 추가

액세스 그룹을 생성하여 다른 관리자에게 특정 시스템, 데스크톱 풀 또는 팜 관리를 위임할 수 있습니다. 기본적으로 데스크톱 풀, 애플리케이션 풀 및 팜은 루트 액세스 그룹에 상주합니다.

루트 액세스 그룹을 포함하여 최대 100개의 액세스 그룹을 가질 수 있습니다.

절차

- 1 Horizon Administrator에서 액세스 그룹 추가 대화 상자로 이동합니다.

옵션	조치
카탈로그에서	<ul style="list-style-type: none"> ■ 카탈로그 > 데스크톱 풀을 선택합니다. ■ 위쪽 창의 액세스 그룹 드롭다운 메뉴에서 새 액세스 그룹을 선택합니다.
리소스에서	<ul style="list-style-type: none"> ■ 리소스 > 팜을 선택합니다. ■ 위쪽 창의 액세스 그룹 드롭다운 메뉴에서 새 액세스 그룹을 선택합니다.
View 구성에서	<ul style="list-style-type: none"> ■ View 구성 > 관리자를 선택합니다. ■ 액세스 그룹 탭에서 액세스 그룹 추가를 선택합니다.

- 2 액세스 그룹의 이름과 설명을 입력하고 **확인**을 클릭합니다.

설명은 선택 사항입니다.

다음에 수행할 작업

하나 이상의 개체를 액세스 그룹으로 이동합니다.

다른 액세스 그룹으로 데스크톱 풀 또는 팜 이동

액세스 그룹을 생성한 후 자동화된 데스크톱 풀, 수동 풀 또는 팜을 새 액세스 그룹으로 이동할 수 있습니다.

절차

- 1 Horizon Administrator에서 **카탈로그 > 데스크톱 풀** 또는 **리소스 > 팜**을 선택합니다.
- 2 풀 또는 팜을 선택합니다.
- 3 상단 창의 액세스 그룹 드롭다운 메뉴에서 액세스 그룹 변경을 선택합니다.
- 4 액세스 그룹을 선택하고 **확인**을 클릭합니다.

Horizon Administrator는 선택된 액세스 그룹으로 풀을 이동합니다.

액세스 그룹 제거

개체가 포함되지 않은 액세스 그룹을 제거할 수 있습니다. 루트 액세스 그룹은 제거할 수 없습니다.

사전 요구 사항

액세스 그룹에 개체가 포함된 경우 다른 액세스 그룹 또는 루트 액세스 그룹으로 개체를 이동합니다. [다른 액세스 그룹으로 데스크톱 풀 또는 팜 이동](#)의 내용을 참조하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 관리자**를 선택합니다.
- 2 **액세스 그룹** 탭에서 액세스 그룹을 선택하고 **액세스 그룹 제거**를 클릭합니다.
- 3 **확인**을 클릭하여 액세스 그룹을 제거합니다.

액세스 그룹의 데스크톱 풀, 애플리케이션 풀 또는 팜 검토

Horizon Administrator에서는 특정 액세스 그룹의 데스크톱 풀, 애플리케이션 풀 또는 팜을 볼 수 있습니다.

절차

- 1 Horizon Administrator에서 개체의 기본 페이지로 이동합니다.

개체	조치
데스크톱 풀	카탈로그 > 데스크톱 풀을 선택합니다.
애플리케이션 풀	카탈로그 > 애플리케이션 풀을 선택합니다.
팜	리소스 > 팜을 선택합니다.

기본적으로 모든 액세스 그룹의 개체가 표시됩니다.

- 2 기본 창의 **액세스 그룹** 드롭다운 메뉴에서 액세스 그룹을 선택합니다.
선택한 액세스 그룹의 개체가 표시됩니다.

액세스 그룹의 vCenter 가상 시스템 검토

Horizon Administrator에서 특정 액세스 그룹의 vCenter 가상 시스템을 검토할 수 있습니다. vCenter 가상 시스템은 해당 풀의 액세스 그룹을 상속합니다.

절차

- 1 Horizon Administrator에서 **리소스 > 시스템**을 선택합니다.
- 2 **vCenter VM** 탭을 선택합니다.

기본적으로 모든 액세스 그룹의 vCenter 가상 시스템이 표시됩니다.

- 3 **액세스 그룹** 드롭다운 메뉴에서 액세스 그룹을 선택합니다.
선택한 액세스 그룹의 vCenter 가상 시스템이 표시됩니다.

사용자 지정 역할 관리

Horizon Administrator를 사용해 사용자 지정 역할을 추가, 수정, 삭제할 수 있습니다.

■ 사용자 지정 역할 추가

미리 정의된 관리자 역할이 사용자 요구에 맞지 않을 경우 특정 권한을 조합해 Horizon Administrator에서 자신만의 고유한 역할을 생성할 수 있습니다.

■ 사용자 지정 역할에서 권한 수정

사용자 지정 역할에서 권한을 수정할 수 있습니다. 미리 정의된 관리자 역할은 수정할 수 없습니다.

■ 사용자 지정 역할 제거

권한에 포함되지 않은 경우 사용자 지정 역할을 제거할 수 있습니다. 미리 정의된 관리자 역할은 제거할 수 없습니다.

사용자 지정 역할 추가

미리 정의된 관리자 역할이 사용자 요구에 맞지 않을 경우 특정 권한을 조합해 Horizon Administrator에서 자신만의 고유한 역할을 생성할 수 있습니다.

사전 요구 사항

사용자 지정 역할 생성 시 사용할 수 있는 관리자 권한을 숙지하십시오. [미리 정의된 역할 및 권한](#) 항목을 참조하십시오.

참고 사용자 지정 관리자 역할을 생성할 때 사용자 지정 관리자 사용자에게는 전역 사용 권한을 사용할 수 없습니다. 미리 정의된 관리자 역할에만 Cloud Pod 아키텍처 환경에서 전역 사용 권한 관리를 사용하도록 설정하는 전역 사용 권한이 있습니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 관리자**를 선택합니다.
- 2 **역할** 탭에서 **역할 추가**를 클릭합니다.
- 3 새 역할의 이름과 설명을 입력하고 권한을 하나 이상 선택한 다음 **확인**을 클릭합니다.
새 역할이 왼쪽 창에 표시됩니다.

사용자 지정 역할에서 권한 수정

사용자 지정 역할에서 권한을 수정할 수 있습니다. 미리 정의된 관리자 역할은 수정할 수 없습니다.

사전 요구 사항

사용자 지정 역할 생성 시 사용할 수 있는 관리자 권한을 숙지하십시오. [미리 정의된 역할 및 권한](#)의 내용을 참조하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 관리자**를 선택합니다.
- 2 **역할** 탭에서 역할을 선택합니다.
- 3 역할의 권한을 표시하려면 **권한**을 클릭하고 **편집**을 클릭합니다.

- 4 권한을 선택 또는 선택 해제하십시오.
- 5 변경 사항을 저장하려면 **확인**을 클릭합니다.

사용자 지정 역할 제거

권한에 포함되지 않은 경우 사용자 지정 역할을 제거할 수 있습니다. 미리 정의된 관리자 역할은 제거할 수 없습니다.

사전 요구 사항

역할이 권한에 포함된 경우 권한을 삭제하십시오. 자세한 내용은 [사용 권한 삭제](#)에 나와 있습니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 관리자**를 선택합니다.
- 2 **역할** 탭에서 역할을 선택하고 **역할 제거**를 클릭합니다.
권한에 포함된 사용자 지정 역할 또는 미리 정의된 역할에는 **역할 제거** 단추를 사용할 수 없습니다.
- 3 역할을 제거하려면 **확인**을 클릭합니다.

미리 정의된 역할 및 권한

Horizon Administrator에는 관리 사용자 및 그룹에 할당할 수 있는 미리 정의된 역할이 포함됩니다. 또한 선택한 권한을 조합하여 고유의 관리자 역할을 생성할 수 있습니다.

- **미리 정의된 관리자 역할**
미리 정의된 관리자 역할은 일반 관리 작업을 수행하기 위해 필요한 모든 개별 권한을 결합시킵니다. 미리 정의된 역할을 수정할 수 없습니다.
- **전역 권한**
전역 권한을 가지고 있으면 전역 설정 보기 및 변경 등과 같은 시스템 차원의 작업을 제어할 수 있습니다. 전역 권한만 포함된 역할은 액세스 그룹에 적용할 수 없습니다.
- **개체 특정 권한**
개체 특정 권한은 특정 유형의 인벤토리 개체에서 작업을 제어합니다. 개체 특정 권한을 포함하는 역할이 액세스 그룹에 적용될 수 있습니다.
- **내부 권한**
일부 미리 정의된 관리자 역할은 특정 내부 권한을 가지고 있습니다. 사용자 지정 역할을 생성하면 내부 권한을 선택할 수 없습니다.

미리 정의된 관리자 역할

미리 정의된 관리자 역할은 일반 관리 작업을 수행하기 위해 필요한 모든 개별 권한을 결합시킵니다. 미리 정의된 역할을 수정할 수 없습니다.

참고 사용자에게 미리 정의된 역할 또는 사용자 지정 역할 조합을 할당하면 미리 정의된 개별 역할 또는 사용자 지정 역할 내에서는 가능하지 않은 작업에 액세스할 수 있게 됩니다.

다음 표에는 미리 정의된 역할이 정리되어 있으며 해당 역할이 액세스 그룹에 적용될 수 있는지 여부를 보여 줍니다.

표 6-6. Horizon Administrator의 미리 정의된 역할

역할	사용자 기능	액세스 그룹에 적용
관리자	<p>추가 관리자 사용자 및 그룹 생성을 포함하여 모든 관리자 작업을 수행합니다. Cloud Pod 아키텍처 환경에서 이 역할을 가진 관리자는 팟 페더레이션을 구성 및 관리하고 원격 팟 세션을 관리할 수 있습니다.</p> <p>루트 액세스 그룹에서 관리자 역할을 가진 관리자는 시스템의 모든 인벤토리 개체에 대해 전체 액세스 권한이 있기 때문에 수퍼유저입니다. 관리자 역할에는 모든 권한이 포함되기 때문에 일부 사용자에게 할당해야 합니다. 처음에는 루트 액세스 그룹에서 연결 서버 호스트의 로컬 관리자 그룹 구성원에게 이 역할이 부여됩니다.</p> <p>중요 다음 작업을 수행하려면 관리자에게 루트 액세스 그룹의 관리자 역할이 있어야 합니다.</p> <ul style="list-style-type: none"> ■ 액세스 그룹을 추가 및 삭제합니다. ■ Horizon Administrator에서 ThinApp 애플리케이션 및 구성 설정을 관리합니다. ■ vdmadmin, vdmimport 및 lmutil 명령을 사용합니다. 	예
관리자(읽기 전용)	<ul style="list-style-type: none"> ■ 전역 설정 및 인벤토리 개체를 보기만 하고 수정하지 않습니다. ■ ThinApp 애플리케이션 및 설정을 보기만 하고 수정하지 않습니다. ■ vdmexport를 포함하지만 vdmadmin, vdmimport 및 lmutil은 제외한 모든 PowerShell 명령 및 명령줄 유틸리티를 실행합니다. <p>Cloud Pod 아키텍처 환경에서 이 역할을 가진 관리자는 전역 데이터 계층의 인벤토리 개체 및 설정을 볼 수 있습니다.</p> <p>관리자가 액세스 그룹에서 이 역할을 가지고 있는 경우 해당 액세스 그룹의 인벤토리 개체만 볼 수 있습니다.</p>	예
에이전트 등록 관리자	물리적 시스템, 독립 실행형 가상 시스템 및 RDS 호스트와 같이 관리되지 않는 시스템을 등록합니다.	아니요
전역 구성 및 정책 관리자	관리자 역할 및 사용 권한을 제외한 전역 정책 및 구성 설정과 ThinApp 애플리케이션 및 설정을 보고 수정할 수 있습니다.	아니요
전역 구성 및 정책 관리자(읽기 전용)	관리자 역할 및 사용 권한을 제외한 전역 정책 및 구성 설정과 ThinApp 애플리케이션 및 설정을 볼 수 있지만 수정하지는 못합니다.	아니요
기술 지원 관리자	<p>종료, 재설정, 다시 시작과 같은 데스크톱 및 애플리케이션 작업을 수행하고, 사용자의 데스크톱 또는 애플리케이션에 대한 프로세스 종료와 같은 원격 지원 작업을 수행합니다. 관리자는 Horizon Help Desk Tool에 액세스하려면 루트 액세스 그룹에 대한 사용 권한이 있어야 합니다.</p> <ul style="list-style-type: none"> ■ Horizon Help Desk Tool에 대한 읽기 전용 액세스 권한입니다. ■ 전역 세션을 관리합니다. ■ Horizon Administrator에 로그인할 수 있습니다. ■ 모든 시스템 및 세션 관련 명령을 수행합니다. ■ 원격 프로세스 및 애플리케이션을 관리합니다. ■ 가상 데스크톱 또는 계시된 데스크톱에 대한 원격 지원입니다. 	아니요

표 6-6. Horizon Administrator의 미리 정의된 역할 (계속)

역할	사용자 기능	액세스 그룹에 적용
기술 지원 관리자(읽기 전용)	<p>사용자 및 세션 정보를 보고 세션 세부 정보에서 드릴다운합니다. 관리자는 Horizon Help Desk Tool에 액세스하려면 루트 액세스 그룹에 대한 사용 권한이 있어야 합니다.</p> <ul style="list-style-type: none"> Horizon Help Desk Tool에 대한 읽기 전용 액세스 권한입니다. Horizon Administrator에 로그인할 수 있습니다. 	아니요
인벤토리 관리자	<ul style="list-style-type: none"> 모든 시스템, 세션 및 풀 관련 작업을 수행합니다. 영구 디스크를 관리합니다. 연결된 클론 풀을 재동기화, 새로 고침 및 재조정하고 기본 풀 이미지를 변경합니다. <p>관리자가 액세스 그룹에서 이 역할을 가지고 있는 경우 해당 액세스 그룹의 인벤토리 개체에 대해서만 이러한 작업을 수행할 수 있습니다.</p>	예
인벤토리 관리자(읽기 전용)	<p>인벤토리 개체를 보기만 하고 수정하지 않습니다.</p> <p>관리자가 액세스 그룹에서 이 역할을 가지고 있는 경우 해당 액세스 그룹의 인벤토리 개체만 볼 수 있습니다.</p>	예
로컬 관리자	<p>추가 관리자 사용자 및 그룹 생성을 제외한 모든 로컬 관리자 작업을 수행합니다. Cloud Pod 아키텍처 환경에서 이 역할을 가진 관리자는 전역 데이터 계층에 대한 작업을 수행하거나 원격 팟의 세션을 관리할 수 없습니다.</p> <p>참고 로컬 관리자 역할을 가진 관리자는 Horizon Help Desk Tool에 액세스할 수 없습니다. CPA가 아닌 환경의 관리자는 Horizon Help Desk Tool에서 작업을 수행하는데 필요한 전역 세션 관리 권한이 없습니다.</p>	예
로컬 관리자(읽기 전용)	<p>전역 데이터 계층의 인벤토리 개체 및 설정 보기를 제외하면 관리자(읽기 전용) 역할과 동일합니다. 이 역할을 가진 관리자는 로컬 팟에서만 읽기 전용 권한을 가집니다.</p> <p>참고 로컬 관리자(읽기 전용) 역할을 가진 관리자는 Horizon Help Desk Tool에 액세스할 수 없습니다. CPA가 아닌 환경의 관리자는 Horizon Help Desk Tool에서 작업을 수행하는데 필요한 전역 세션 관리 권한이 없습니다.</p>	예

전역 권한

전역 권한을 가지고 있으면 전역 설정 보기 및 변경 등과 같은 시스템 차원의 작업을 제어할 수 있습니다. 전역 권한만 포함된 역할은 액세스 그룹에 적용할 수 없습니다.

다음 표에서는 전역 권한을 설명하고 각 권리를 포함하는 미리 정의된 역할 목록을 보여 줍니다.

표 6-7. 전역 권한

권한	사용자 기능	미리 정의된 역할
콘솔 상호 작용	Horizon Administrator에 로그인하고 사용합니다.	관리자 관리자(읽기 전용) 인벤토리 관리자 인벤토리 관리자(읽기 전용) 전역 구성 및 정책 관리자 전역 구성 및 정책 관리자(읽기 전용) 기술 지원 관리자 기술 지원 관리자(읽기 전용) 로컬 관리자 로컬 관리자(읽기 전용)
직접 상호 작용	vdmadmin 및 vdmimport를 제외한 모든 PowerShell 명령과 명령줄 유틸리티를 실행합니다. vdmadmin, vdmimport 및 lmutil 명령을 사용하려면 관리자가 루트 액세스 그룹에 대한 관리자 역할을 가지고 있어야 합니다.	관리자 관리자(읽기 전용)
전역 구성 및 정책 관리	관리자 역할 및 사용 권한을 제외한 전역 정책 및 구성 설정을 보고 수정합니다.	관리자 전역 구성 및 정책 관리자
전역 세션 관리	Cloud Pod 아키텍처 환경에서 전역 세션을 관리합니다.	관리자
역할 및 사용 권한 관리	관리자 역할 및 사용 권한을 생성, 수정, 삭제합니다.	관리자
에이전트 등록	물리적 시스템, 독립 실행형 가상 시스템 및 RDS 호스트 같은 관리되지 않는 시스템에 Horizon Agent를 설치합니다. Horizon Agent를 설치하는 동안 연결 서버 인스턴스에 관리되지 않는 시스템을 등록하려면 관리자 로그인 자격 증명을 입력해야 합니다.	관리자 에이전트 등록 관리자

개체 특정 권한

개체 특정 권한은 특정 유형의 인벤토리 개체에서 작업을 제어합니다. 개체 특정 권한을 포함하는 역할이 액세스 그룹에 적용될 수 있습니다.

다음 표에서는 개체별 권한에 대해 설명합니다. 미리 정의된 역할 관리자 및 인벤토리 관리자에는 이러한 모든 권한이 포함됩니다.

표 6-8. 개체 특정 권한

권한	사용자 기능	개체
팝 및 데스크톱 풀 사용	데스크톱 풀을 사용하거나 사용하지 않도록 설정합니다.	데스크톱 풀, 팝
데스크톱 및 애플리케이션 풀 권한 부여	사용자 권한을 추가 및 제거합니다.	데스크톱 풀, 애플리케이션 풀
Composer 데스크톱 풀 이미지 관리	연결된 클론 풀을 재동기화, 새로 고침 및 재조정하고 기본 풀 이미지를 변경합니다.	데스크톱 풀

표 6-8. 개체 특정 권한 (계속)

권한	사용자 기능	개체
시스템 관리	모든 시스템 및 세션 관련 작업을 수행합니다.	시스템
영구 디스크 관리	영구 데스크 연결, 분리 및 가져오기를 포함하여 모든 View Composer 영구 디스크 작업을 수행합니다.	영구 디스크
팜과 데스크톱 및 애플리케이션 풀 관리	팜을 추가, 수정 및 삭제합니다. 데스크톱과 애플리케이션 풀을 추가, 수정 및 삭제하고 권한을 부여합니다. 시스템을 추가 및 제거합니다.	데스크톱 풀, 애플리케이션 풀, 팜
세션 관리	세션 연결을 끊고 로그오프하여 사용자에게 메시지를 보냅니다.	세션
재부팅 작업 관리	가상 시스템을 재설정하거나 가상 데스크톱을 다시 시작합니다.	시스템

내부 권한

일부 미리 정의된 관리자 역할은 특정 내부 권한을 가지고 있습니다. 사용자 지정 역할을 생성하면 내부 권한을 선택할 수 없습니다.

다음 표에서는 내부 권한을 설명하고 각 권한을 포함하는 미리 정의된 역할 목록을 보여 줍니다.

표 6-9. 내부 권한

권한	설명	미리 정의된 역할
전체(읽기 전용)	모든 설정에 대한 읽기 전용 액세스 권한을 부여합니다.	관리자(읽기 전용)
인벤토리 관리(읽기 전용)	인벤토리 개체에 읽기 전용 액세스 권한을 부여합니다.	인벤토리 관리자(읽기 전용)
전역 구성 및 정책 관리(읽기 전용)	관리자 및 사용자를 제외한 구성 설정 및 전역 정책에 읽기 전용 액세스 권한을 부여합니다.	전역 구성 및 정책 관리자(읽기 전용)

일반 작업에 필요한 권한

많은 일반 관리 작업에는 통합된 권한 집합이 필요합니다. 일부 작업에는 조작할 개체에 대한 액세스 권한 외에도 루트 액세스 그룹의 권한이 필요합니다.

풀 관리 권한

관리자는 Horizon Administrator에서 풀을 관리하기 위한 특정 권한을 가지고 있어야 합니다.

다음 표에는 일반 풀 관리 작업이 나열되어 있고 각 작업을 수행하는 데 필요한 권한이 나와 있습니다.

표 6-10. 풀 관리 작업 및 권한

작업	필수 권한
데스크톱 풀 사용 또는 사용 안 함	팜 및 데스크톱 풀 사용
사용자에게 풀에 대한 권한 부여 또는 해제	데스크톱 및 애플리케이션 풀 권한 부여
풀 추가	팜과 데스크톱 및 애플리케이션 풀 관리

표 6-10. 풀 관리 작업 및 권한 (계속)

작업	필수 권한
풀 수정 또는 삭제	팜과 데스크톱 및 애플리케이션 풀 관리
풀에서 데스크톱 추가 또는 제거	팜과 데스크톱 및 애플리케이션 풀 관리
기본 View Composer 이미지 새로 고침, 재구성, 재조정 또는 변경	Composer 데스크톱 풀 이미지 관리
액세스 그룹 변경	소스와 대상 액세스 그룹 모두에서 팜과 데스크톱 및 애플리케이션 풀 관리

시스템 관리 권한

관리자는 Horizon Administrator에서 시스템을 관리하기 위한 특정 권한을 가지고 있어야 합니다. 다음 표에는 일반 시스템 관리 작업이 나열되어 있고 각 작업을 수행하는 데 필요한 권한이 나와 있습니다.

표 6-11. 시스템 관리 작업 및 권한

작업	필수 권한
가상 시스템 제거	시스템 관리
가상 시스템 재설정	재부팅 작업 관리
가상 데스크톱 다시 시작	재부팅 작업 관리
사용자 할당 또는 제거	시스템 관리
유지 관리 모드 시작 또는 종료	시스템 관리
세션 연결 끊기 또는 로그오프	세션 관리

영구 디스크 관리 권한

관리자는 Horizon Administrator에서 영구 디스크를 관리하기 위한 특정 권한을 가지고 있어야 합니다.

다음 표에는 일반 영구 디스크 관리 작업이 나열되어 있고 각 작업을 수행하는 데 필요한 권한이 나와 있습니다. Horizon Administrator의 영구 디스크 페이지에서 이러한 작업을 수행합니다.

표 6-12. 영구 디스크 관리 작업 및 권한

작업	필수 권한
디스크 분리	디스크에 대한 영구 디스크 관리 및 풀에 대한 팜과 데스크톱 및 애플리케이션 풀 관리
디스크 연결	디스크에 대한 영구 디스크 관리 및 시스템에 대한 팜과 데스크톱 및 애플리케이션 풀 관리
디스크 편집	디스크에 대한 영구 디스크 관리 및 선택한 풀에 대한 팜과 데스크톱 및 애플리케이션 풀 관리
액세스 그룹 변경	소스 및 대상 액세스 그룹에 대한 영구 디스크 관리

표 6-12. 영구 디스크 관리 작업 및 권한 (계속)

작업	필수 권한
데스크톱 재생성	디스크에 대한 영구 디스크 관리 및 마지막 풀에 대한 팜과 데스크톱 및 애플리케이션 풀 관리
vCenter에서 가져오기	폴더에 대한 영구 디스크 관리 및 풀에 대한 풀 관리
디스크 삭제	디스크에 대한 영구 디스크 관리

사용자 및 관리자 관리 권한

관리자는 Horizon Administrator에서 사용자 및 관리자를 관리하기 위한 특정 권한을 가지고 있어야 합니다.

다음 표에는 일반 사용자 및 관리자 관리 작업이 나열되어 있고 각 작업을 수행하는 데 필요한 권한이 나와 있습니다. Horizon Administrator의 사용자 및 그룹 페이지에서 사용자를 관리합니다. Horizon Administrator의 전역 관리자 보기 페이지에서 관리자를 관리합니다.

표 6-13. 사용자 및 관리자 관리 작업 및 권한

작업	필수 권한
일반 사용자 정보 업데이트	전역 구성 및 정책 관리
사용자에게 메시지 보내기	시스템의 원격 세션 관리
관리자 사용자 또는 그룹 추가	역할 및 사용 권한 관리
관리자 권한 추가, 수정 또는 삭제	역할 및 사용 권한 관리
관리자 역할 추가, 수정 또는 삭제	역할 및 사용 권한 관리

Horizon Help Desk Tool 작업에 대한 권한

Horizon Help Desk Tool 관리자는 Horizon Administrator에서 문제 해결 작업 수행하기 위한 특정 권한이 있어야 합니다.

다음 표에는 Horizon Help Desk Tool 관리자가 수행할 수 있는 일반적인 작업과 각 작업을 수행하기 위한 권한이 나와 있습니다.

표 6-14. Horizon Help Desk Tool 작업 및 권한

작업	필수 권한
Horizon Help Desk Tool에 대한 읽기 전용 액세스 권한입니다.	헬프 데스크 관리(읽기 전용)
전역 세션을 관리합니다.	전역 세션 관리
Horizon Administrator에 로그인할 수 있습니다.	콘솔 상호 작용
모든 시스템 및 세션 관련 명령을 수행합니다.	시스템 관리
시스템을 재설정하거나 다시 시작합니다.	재부팅 작업 관리
세션 연결을 끊고 로그오프합니다.	세션 관리
원격 프로세스 및 애플리케이션을 관리합니다.	원격 프로세스 및 애플리케이션 관리

표 6-14. Horizon Help Desk Tool 작업 및 권한 (계속)

작업	필수 권한
가상 데스크톱 또는 게시된 데스크톱에 대한 원격 지원입니다.	원격 지원
전역 세션에 대해 연결 끊기, 로그오프, 재설정 및 다시 시작 작업을 수행합니다.	헬프 데스크 관리(읽기 전용) 및 전역 세션 관리
로컬 세션에 대해 재설정 및 다시 시작 작업을 수행합니다.	헬프 데스크 관리(읽기 전용) 및 재부팅 작업 관리
원격 지원 작업입니다.	헬프 데스크 관리(읽기 전용) 및 원격 지원
원격 프로세스 및 애플리케이션을 종료합니다.	헬프 데스크 관리(읽기 전용) 및 원격 프로세스 및 애플리케이션 관리
Horizon Help Desk Tool에서 모든 작업을 수행합니다.	헬프 데스크 관리(읽기 전용), 전역 세션 관리, 재부팅 작업 관리, 원격 지원 및 원격 프로세스 및 애플리케이션 관리
원격 지원 작업을 수행하고 원격 프로세스 및 애플리케이션을 종료합니다.	헬프 데스크 관리(읽기 전용), 원격 지원 및 원격 프로세스 및 애플리케이션 관리
로컬 세션에 대해 연결 해제 및 로그오프 작업을 수행합니다.	헬프 데스크 관리(읽기 전용) 및 세션 관리

일반 관리 작업 및 명령 권한

관리자는 일반 관리 작업을 수행하고 명령줄 유틸리티를 실행하기 위한 특정 권한이 있어야 합니다.

다음 표에는 일반 관리 작업을 수행하고 명령줄 유틸리티를 실행하는 데 필요한 권한이 나와 있습니다.

표 6-15. 일반 관리 작업 및 명령 권한

작업	필수 권한
액세스 그룹 추가 또는 삭제	루트 액세스 그룹에 대한 관리자 역할이 있어야 합니다.
Horizon Administrator에서 ThinApp 애플리케이션 및 설정 관리	루트 액세스 그룹에 대한 관리자 역할이 있어야 합니다.
물리적 시스템, 독립 실행형 가상 시스템 또는 RDS 호스트와 같은 관리되지 않는 시스템에 Horizon Agent 설치	에이전트 등록
Horizon Administrator에서 관리 설정 보기 또는 수정 (관리자 제외)	전역 구성 및 정책 관리
vdmadmin 및 vdmimport를 제외한 모든 PowerShell 명령과 명령줄 유틸리티를 실행합니다.	직접 상호 작용
vdmadmin 및 vdmimport 명령 사용	루트 액세스 그룹에 대한 관리자 역할이 있어야 합니다.
vdmexport 명령 사용	루트 액세스 그룹에 대한 관리자 역할 또는 관리자(읽기 전용) 역할이 있어야 합니다.

관리자 사용자 및 그룹의 모범 사례

Horizon 7 환경의 보안과 관리 효율성을 향상하려면 모범 사례에 따라 관리자 사용자 및 그룹을 관리해야 합니다.

- Active Directory에 새 사용자 그룹을 생성하고 해당 그룹에 관리 역할을 할당하십시오. Windows 기본 제공 그룹 또는 Horizon 7 권한이 필요하지 않거나 없어야 하는 사용자가 포함될 수 있는 다른 기존 그룹을 사용하지 마십시오.
- Horizon 7 관리 권한이 있는 사용자 수는 최소한으로 유지하십시오.
- 관리자 역할은 모든 권한을 가지고 있으므로 일상적인 관리에 사용하면 안 됩니다.
- 관리자 이름은 매우 쉽게 확인하고 추정할 수 있으므로 관리자 사용자 및 그룹을 생성할 때 이 이름을 사용하지 마십시오.
- 액세스 그룹을 생성하여 중요한 데스크톱과 팜을 분리하십시오. 이들 액세스 그룹 관리를 제한된 사용자 집합에 위임하십시오.
- 전역 정책과 Horizon 7 구성 설정을 수정할 수 있는 관리자를 별도로 생성하십시오.

Horizon Administrator 및 Active Directory에서 정책 구성

7

Horizon Administrator를 사용하여 클라이언트 세션의 정책을 설정할 수 있습니다. View 연결 서버의 동작, PCoIP 디스플레이 프로토콜 및 Horizon 7 로깅 및 성능 경보를 제어하기 위해 Active Directory 그룹 정책 설정을 구성할 수 있습니다.

그뿐만 아니라 Active Directory 그룹 정책 설정을 구성하여 Horizon Agent, Windows용 Horizon Client, Horizon Persona Management 및 특정 기능의 동작을 제어할 수도 있습니다. 이러한 정책 설정에 대한 자세한 내용은 Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [Horizon Administrator에서 정책 설정](#)
- [Horizon 7 그룹 정책 관리 템플릿 파일 사용](#)

Horizon Administrator에서 정책 설정

클라이언트 세션의 정책은 Horizon Administrator를 사용하여 구성합니다.

이러한 정책을 설정하여 특정 사용자, 특정 데스크톱 풀 또는 모든 클라이언트 세션 사용자에게 영향을 줄 수 있습니다. 특정 사용자 및 데스크톱 풀에 영향을 주는 정책을 사용자 수준 정책 및 데스크톱 풀 수준 정책이라고 합니다. 모든 세션 및 사용자에게 영향을 주는 정책은 전역 정책이라고 합니다.

사용자 수준 정책은 동등한 데스크톱 풀 수준 정책 설정에서 설정을 상속합니다. 마찬가지로 데스크톱 풀 수준 정책은 동등한 전역 정책 설정에서 설정을 상속합니다. 데스크톱 풀 수준 정책 설정은 동등한 전역 정책 설정보다 우선합니다. 사용자 수준 정책 설정은 동등한 전역 및 데스크톱 풀 수준 정책 설정보다 우선합니다.

낮은 수준의 정책 설정은 동일한 높은 수준의 설정보다 더 또는 덜 제한적일 수 있습니다. 예를 들어, 전역 정책을 **거부**로 설정하고 동등한 데스크톱 풀 수준 정책을 **허용**으로 설정할 수 있으며, 그 반대도 가능합니다.

참고 게시된 데스크톱 및 애플리케이션 풀에 대해 전역 정책만 사용할 수 있습니다. 게시된 데스크톱 및 애플리케이션 풀에 대해 사용자 수준 정책이나 풀 수준 정책을 설정할 수 없습니다.

■ 전역 정책 설정 구성

전역 정책을 구성해 모든 클라이언트 세션 사용자의 동작을 제어할 수 있습니다.

■ 데스크톱 풀 정책 구성

특정 데스크톱 풀에 적용할 데스크톱 수준 정책을 구성할 수 있습니다. 데스크톱 수준 정책 설정은 동등한 전역 정책 설정보다 우선합니다.

■ 사용자를 위한 정책 구성

특정 사용자에게 적용할 사용자 수준 정책을 구성할 수 있습니다. 사용자 수준 정책 설정은 동등한 전역과 데스크톱 풀 수준 정책 설정보다 항상 우선합니다.

■ Horizon 7 정책

모든 클라이언트 세션에 영향을 주는 Horizon 7 정책을 구성하거나 특정 데스크톱 풀 또는 사용자에게 영향을 주도록 정책을 적용할 수 있습니다.

전역 정책 설정 구성

전역 정책을 구성해 모든 클라이언트 세션 사용자의 동작을 제어할 수 있습니다.

사전 요구 사항

정책 설명을 숙지하십시오. [Horizon 7 정책](#)를 참조하십시오.

절차

- 1 Horizon Administrator에서 **정책 > 전역 정책**을 선택합니다.
- 2 **View 정책** 창에서 **정책 편집**을 클릭합니다.
- 3 변경 사항을 저장하려면 **확인**을 클릭합니다.

데스크톱 풀 정책 구성

특정 데스크톱 풀에 적용할 데스크톱 수준 정책을 구성할 수 있습니다. 데스크톱 수준 정책 설정은 동등한 전역 정책 설정보다 우선합니다.

사전 요구 사항

정책 설명을 숙지하십시오. [Horizon 7 정책](#)를 참조하십시오.

절차

- 1 Horizon Administrator에서 **카탈로그 > 데스크톱 풀**을 선택합니다.
- 2 데스크톱 풀 ID를 두 번 클릭하고 **정책** 탭을 클릭합니다.
정책 탭은 현재 정책 설정을 표시합니다. 동등한 전역 설정에서 설정을 상속한 경우에는 **데스크톱 풀 정책** 옆에 **상속**이 표시됩니다.
- 3 **View 정책** 창에서 **정책 편집**을 클릭합니다.
- 4 변경 사항을 저장하려면 **확인**을 클릭합니다.

사용자를 위한 정책 구성

특정 사용자에게 적용할 사용자 수준 정책을 구성할 수 있습니다. 사용자 수준 정책 설정은 동등한 전역과 데스크톱 풀 수준 정책 설정보다 항상 우선합니다.

사전 요구 사항

정책 설명을 숙지하십시오. [Horizon 7 정책](#)를 참조하십시오.

절차

- 1 Horizon Administrator에서 **카탈로그 > 데스크톱 풀**을 선택합니다.
- 2 데스크톱 풀 ID를 두 번 클릭하고 **정책** 탭을 클릭합니다.

정책 탭은 현재 정책 설정을 표시합니다. 동등한 전역 설정에서 설정을 상속한 경우에는 **데스크톱 풀 정책** 옆에 **상속**이 표시됩니다.
- 3 **사용자 재정의**를 클릭한 다음 **사용자 추가**를 클릭합니다.
- 4 사용자를 찾으려면 **추가**를 클릭하고 사용자 이름 또는 설명을 입력한 다음 **찾기**를 클릭합니다.
- 5 목록에서 사용자를 한 명 이상 선택하고 **확인**을 클릭한 후 **다음**을 클릭합니다.
 개별 정책 추가 대화 상자가 나타납니다.
- 6 Horizon 정책을 구성하고 **마침**을 클릭하여 변경 내용을 저장합니다.

Horizon 7 정책

모든 클라이언트 세션에 영향을 주는 Horizon 7 정책을 구성하거나 특정 데스크톱 풀 또는 사용자에게 영향을 주도록 정책을 적용할 수 있습니다.

다음 표에서는 각 Horizon 7 정책 설정에 대해 설명합니다.

표 7-1. Horizon 정책

정책	설명
MMR(멀티미디어 리디렉션)	<p>클라이언트 시스템을 위해 MMR이 사용되도록 설정되어 있는지 확인합니다.</p> <p>MMR은 TCP 소켓을 통해 직접 원격 데스크톱의 특정 코덱에서 멀티미디어 데이터를 클라이언트 시스템에 전달하는 Windows Media Foundation 필터입니다. 그런 다음 데이터는 재생되는 클라이언트 시스템에서 바로 디코딩됩니다.</p> <p>기본값은 거부입니다.</p> <p>클라이언트 시스템에 로컬 멀티미디어 디코딩을 처리하는 리소스가 충분하지 않은 경우 거부 설정을 그대로 둡니다.</p> <p>멀티미디어 리디렉션(MMR) 데이터는 애플리케이션 기준 암호화 없이 네트워크를 통해 전송되며 리디렉션되는 콘텐츠에 따라 중요한 데이터가 포함될 수 있습니다. 이 데이터가 네트워크에서 모니터링되는 것을 방지하려면 보안 네트워크 상에서만 MMR을 사용하십시오.</p>
USB 액세스	<p>원격 데스크톱에서 클라이언트 시스템에 연결된 USB 디바이스를 사용할 수 있는지 여부를 결정합니다.</p> <p>기본값은 허용입니다. 보안상의 이유를 위해 외부 디바이스의 사용을 막으려면 설정을 거부로 변경하십시오.</p>
PCoIP 하드웨어 가속	<p>PCoIP 디스플레이 프로토콜의 하드웨어 가속을 사용하도록 설정할지 여부를 확인하고 PCoIP 사용자 세션에 할당된 가속 우선 순위를 지정합니다.</p> <p>이 설정은 PCoIP 하드웨어 가속 디바이스가 원격 데스크톱을 호스팅하는 물리적 컴퓨터에 있는 경우에만 적용됩니다.</p> <p>기본값은 중간 우선 순위에서 허용입니다.</p>

Horizon 7 그룹 정책 관리 템플릿 파일 사용

Horizon 7에서는 몇 가지 구성 요소 관련 그룹 정책 관리 ADMX 템플릿 파일을 제공합니다. ADMX 템플릿 파일의 정책 설정을 Active Directory의 새 GPO 또는 기존 GPO에 추가하여 원격 데스크톱 및 애플리케이션을 최적화하고 보호할 수 있습니다.

Horizon 7에 대한 그룹 정책 설정을 제공하는 모든 ADMX 파일은 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyy.zip에 있습니다. 여기서 x.x.x는 버전이고 yyyyyyy는 빌드 번호입니다.

<https://my.vmware.com/web/vmware/downloads>의 VMware 다운로드 사이트에서 파일을 다운로드할 수 있습니다. Desktop & End-User Computing에서 ZIP 파일이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

Horizon 7 ADMX 템플릿 파일에는 컴퓨터 구성 및 사용자 구성 그룹 정책 모두가 포함됩니다.

- 컴퓨터 구성 정책은 데스크톱에 연결하는 사용자에게 관계없이 모든 원격 데스크톱에 적용되는 정책을 설정합니다.
- 사용자 구성 정책은 사용자가 연결하는 원격 데스크톱 또는 애플리케이션에 관계없이 모든 사용자에게 적용할 정책을 설정합니다. 사용자 구성 정책은 동일한 컴퓨터 구성 정책보다 우선합니다.

Microsoft Windows는 데스크톱이 시작될 때와 사용자가 로그인할 때 정책을 적용합니다.

Horizon 7 ADMX 템플릿 파일

Horizon 7 ADMX 템플릿 파일은 Horizon 7 구성 요소를 제어하고 최적화하기 위한 그룹 정책 설정을 제공합니다.

ADMX 파일은 VMware 다운로드 사이트

<https://my.vmware.com/web/vmware/downloads>에서 사용할 수 있는 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip에 있습니다. Desktop & End-User Computing에서 ZIP 파일이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

표 7-2. Horizon ADMX 템플릿 파일

템플릿 이름	템플릿 파일	설명
VMware View Agent 구성	vdm_agent.admx	Horizon Agent의 환경 구성 요소 및 인증과 관련된 정책 설정이 포함됩니다. Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.
VMware Horizon Client 구성	vdm_client.admx	Windows용 Horizon Client와 관련된 정책 설정이 들어 있습니다. 연결 서버 호스트 도메인 외부에서 연결하는 클라이언트는 Horizon Client에 적용된 정책의 영향을 받지 않습니다. Windows용 VMware Horizon Client 설치 및 설정 가이드 문서를 참조하십시오.
VMware Horizon URL 리디렉션	urlRedirection.admx	URL 콘텐츠 리디렉션 기능과 관련된 정책 설정이 포함되어 있습니다. 이 템플릿을 원격 데스크톱 풀 또는 애플리케이션 풀의 GPO에 추가하면 원격 데스크톱이나 애플리케이션 내부에서 클릭하는 특정 URL 링크를 Windows 기반 클라이언트로 리디렉션하고 클라이언트 측 브라우저에서 열 수 있습니다. 이 템플릿을 클라이언트 측 GPO에 추가하면, 사용자가 Windows 기반 클라이언트 시스템에서 특정 URL을 클릭할 때 해당 URL을 원격 데스크톱이나 애플리케이션에서 열 수 있습니다. Horizon 7에서 원격 데스크톱 기능 구성 문서 및 Windows용 VMware Horizon Client 설치 및 설정 가이드 문서를 참조하십시오.
VMware View Server 구성	vdm_server.admx	연결 서버와 관련된 정책 설정이 포함됩니다.
VMware View 일반 구성	vdm_common.admx	모든 Horizon 구성 요소에 일반적인 정책 설정이 포함됩니다.
PCoIP 세션 변수	pcoip.admx	PCoIP 디스플레이 프로토콜과 관련된 정책 설정이 들어 있습니다. Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.
PCoIP 클라이언트 세션 변수	pcoip.client.admx	Windows용 Horizon Client에 영향을 주는 PCoIP 디스플레이 프로토콜과 관련된 정책 설정이 들어 있습니다. Windows용 VMware Horizon Client 설치 및 설정 가이드 문서를 참조하십시오.
개인 설정 관리	ViewPM.admx	Horizon Persona Management와 관련된 정책 설정이 포함되어 있습니다. Horizon 7에서 가상 데스크톱 설정 문서를 참조하십시오.

표 7-2. Horizon ADMX 템플릿 파일 (계속)

템플릿 이름	템플릿 파일	설명
VMware 가상 인쇄 리디렉션	printerRedirection.admx	위치 기반 인쇄를 사용하지 않도록 설정하고, 인쇄 설정 지속성을 사용하지 않도록 설정하고, 리디렉션된 클라이언트 프린터의 프린터 드라이버를 선택하기 위한 정책 설정이 포함되어 있습니다.
위치 기반 인쇄	LBP.xml	VMware 가상 인쇄의 각 위치 기반 프린터에 대한 변환 규칙을 정의하는 템플릿입니다.
원격 데스크톱 서비스	vmware_rds_server.admx	원격 데스크톱 서비스와 관련된 정책 설정이 들어 있습니다. Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.
View RTAV 구성	vdm_agent_rtav.admx	실시간 오디오-비디오 기능과 함께 사용되는 웹캠과 관련된 정책 설정이 포함되어 있습니다. Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.
스캐너 리디렉션	vdm_agent_scanner.admx	게시된 데스크톱 및 애플리케이션에서 사용하기 위해 리디렉션되는 스캔 디바이스와 관련된 정책 설정이 포함되어 있습니다. Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.
직렬 COM	vdm_agent_serialport.admx	가상 데스크톱에서 사용하기 위해 리디렉션되는 직렬(COM) 포트와 관련된 정책 설정이 포함되어 있습니다. Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.
VMware Horizon 프린터 리디렉션	vdm_agent_printing.admx	리디렉션된 프린터 필터링과 관련된 정책 설정이 포함되어 있습니다. Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.
View Agent Direct-Connection	view_agent_direct_connection.admx	View Agent Direct-Connection 플러그인과 관련된 정책 설정이 포함되어 있습니다. View Agent Direct-Connection 플러그인 관리 문서를 참조하십시오.
VMware Horizon 성능 추적기	perf_tracker.admx	VMware Horizon 성능 추적기 기능과 관련된 정책 설정이 포함되어 있습니다. VMware Horizon 성능 추적기 사용 의 내용을 참조하십시오.
VMware Horizon Client 드라이브 리디렉션	vdm_agent_cdr.admx	클라이언트 드라이브 리디렉션 기능과 관련된 정책 설정이 포함되어 있습니다. Horizon 7에서 원격 데스크톱 기능 구성 문서를 참조하십시오.

Horizon 연결 서버 구성 ADMX 템플릿 설정

View Server 구성 ADMX(vdm_server.admx) 템플릿 파일에는 모든 Horizon 연결 서버와 관련된 정책 설정이 포함되어 있습니다.

다음 표에는 연결 서버 구성 ADMX 템플릿 파일의 각 정책 설정에 대해 설명되어 있습니다. 템플릿에는 Computer Configuration 설정만 포함됩니다. 모든 설정은 그룹 정책 관리 편집기의 **컴퓨터 구성 > 정책 > 관리 템플릿 > VMware View Server 구성** 폴더에 있습니다.

표 7-3. Horizon Server 구성 템플릿 설정

설정	속성
Enumerate Forest Trust Child Domains	<p>서버가 상주하는 도메인이 신뢰하는 모든 도메인이 열거되는지 확인합니다. 완전한 신뢰 체인을 설정하기 위해 각 신뢰된 도메인에서 신뢰하는 도메인 또한 열거되고 모든 신뢰된 도메인을 찾을 때까지 프로세스가 재귀적으로 계속됩니다. 로그인 시 모든 신뢰된 도메인을 클라이언트에 사용할 수 있도록 이 정보가 연결 서버에 전달됩니다.</p> <p>이 속성은 기본적으로 사용하도록 설정됩니다. 사용되지 않도록 설정된 경우, 직접 신뢰된 도메인만 열거되며 원격 도메인 컨트롤러에 연결되지 않습니다.</p> <p>참고 복합 도메인 관계를 가진 환경에서(예: 포리스트의 도메인 사이에서 신뢰된 여러 포리스트 구조를 사용) 프로세스 완료에는 몇 분이 걸릴 수 있습니다.</p>
Recursive Enumeration of Trusted Domains	<p>서버가 상주하는 도메인이 신뢰하는 모든 도메인이 열거되는지 확인합니다. 완전한 신뢰 체인을 설정하기 위해 각 신뢰된 도메인에서 신뢰하는 도메인 또한 열거되고 모든 신뢰된 도메인을 찾을 때까지 재귀적으로 프로세스를 계속합니다. 로그인 시 모든 신뢰된 도메인을 클라이언트에 사용할 수 있도록 이 정보가 View 연결 서버에 전달됩니다.</p> <p>이 설정은 기본적으로 사용하도록 설정됩니다. 사용되지 않도록 설정된 경우, 직접 신뢰된 도메인만 열거되며 원격 도메인 컨트롤러에 연결되지 않습니다.</p> <p>복합 도메인 관계를 가진 환경에서(예: 포리스트의 도메인 사이에서 신뢰된 여러 포리스트 구조를 사용) 이 프로세스 완료에는 몇 분이 걸릴 수 있습니다.</p>
Windows Password Authentication Mode	<p>Windows 암호 인증 모드를 선택합니다.</p> <ul style="list-style-type: none"> ■ KerberosOnly. Kerberos를 사용하여 인증합니다. ■ KerberosWithFallbackToNTLM. Kerberos를 사용하여 인증하지만 실패 시 NTLM 사용으로 폴백합니다. ■ Legacy. NTLM을 사용하여 인증하지만 실패 시 Kerberos 사용으로 폴백합니다. 레거시 NT 도메인 컨트롤러를 지원하는 데 사용됩니다. 기본값은 KerberosOnly입니다.

Horizon 7 일반 구성 ADMX 템플릿 설정

Horizon 7 일반 구성 ADMX(vdm_common.admx) 템플릿 파일에는 모든 Horizon 구성 요소에 공통되는 정책 설정이 포함되어 있습니다. 이러한 템플릿에는 컴퓨터 구성 설정만 포함됩니다.

로그 구성 설정

다음 표에는 Horizon 일반 구성 ADMX 템플릿 파일의 로그 구성 정책 설정에 대해 설명되어 있습니다. 모든 설정은 그룹 정책 관리 편집기의 **컴퓨터 구성 > 정책 > 관리 템플릿 > VMware View 일반 구성 > 로그 구성** 폴더에 있습니다.

표 7-4. View 일반 구성 템플릿: 로그 구성 설정

설정	속성
Number of days to keep production logs	로그 파일이 시스템에 유지되는 일수를 지정합니다. 설정된 값이 없는 경우, 기본값이 적용되며 7일간 로그 파일이 보관됩니다.
Maximum number of debug logs	시스템에 유지할 디버그 로그 파일의 최대 수를 지정합니다. 로그 파일이 최대 크기에 도달할 경우, 더 이상의 항목이 추가되지 않고 새 로그 파일이 생성됩니다. 이전 로그 파일 수가 이 값에 도달할 경우, 가장 오래된 로그 파일이 삭제됩니다.
Maximum debug log size in Megabytes	로그 파일이 닫히고 새 로그 파일이 생성되기 전에 디버그 로그가 도달할 수 있는 최대 크기(MB 단위)를 지정합니다.
Log Directory	로그 파일의 디렉토리에 대한 전체 경로를 지정합니다. 위치를 쓸 수 없는 경우, 기본 위치가 사용됩니다. 클라이언트 로그 파일의 경우, 클라이언트 이름이 있는 임시 디렉토리가 생성됩니다.
Send logs to a Syslog server	<p>VMware vCenter Log Insight 등의 Syslog 서버에 View Server 로그를 보낼 수 있습니다. 로그는 이 GPO가 구성된 OU 또는 도메인의 모든 View Server에서 전송됩니다.</p> <p>데스크톱이 포함된 OU에 연결된 GPO에서 이 설정을 사용하도록 설정하여 Syslog 서버에 Horizon Agent 로그를 보낼 수 있습니다.</p> <p>Syslog 서버에 로그 데이터를 보내려면 이 설정을 사용하도록 설정하고 로그 수준과 서버의 정규화된 도메인 이름(FQDN) 또는 IP 주소를 지정하십시오. 기본 포트 514를 사용하지 않을 경우 대체 포트를 지정할 수 있습니다. 지정할 때는 각 요소를 세로 막대()로 구분하십시오. 다음 구문을 사용하십시오.</p> <p>Log Level Server FQDN or IP [Port number(514 default)]</p> <p>예: Debug 192.0.2.2</p> <p>중요 Syslog 데이터는 소프트웨어 기반 암호화 없이 네트워크를 통해 전송됩니다. 중요한 데이터가 View Server 로그에 포함될 수 있으므로 안전하지 않은 네트워크에서는 Syslog 데이터 전송을 피하십시오. 가능하면 IPsec과 같은 링크 계층 보안을 사용하여 이 데이터가 네트워크에서 모니터링될 가능성을 차단하십시오.</p>

성능 알람 설정

표 7-5에는 Horizon 일반 구성 ADMX 템플릿 파일의 성능 알람 설정에 대해 설명되어 있습니다. 모든 설정은 그룹 정책 관리 편집기의 **컴퓨터 구성 > 정책 > 관리 템플릿 > VMware View 일반 구성 > 성능 알람** 폴더에 있습니다.

표 7-5. View 일반 구성 템플릿: 성능 알람 설정

설정	속성
CPU and Memory Sampling Interval in Seconds	CPU 및 메모리 폴링 간격 CPU를 지정합니다. 샘플링 간격이 낮아지면 로그에 대한 출력 수준이 높아집니다.
Overall CPU usage percentage to issue log info	시스템의 전체 CPU 사용이 로그되는 임계값을 지정합니다. 여러 프로세서를 사용할 수 있는 경우, 이 백분율은 조합된 사용량을 나타냅니다.
Overall memory usage percentage to issue log info	커밋된 전체 시스템 메모리 사용이 로그되는 임계값을 지정합니다. 커밋된 시스템 메모리는 프로세서에서 할당하고 운영 체제가 물리적 메모리를 또는 페이지 파일의 페이지 슬롯을 커밋한 메모리입니다.

표 7-5. View 일반 구성 템플릿: 성능 알람 설정 (계속)

설정	속성
Process CPU usage percentage to issue log info	임의 개별 프로세스의 CPU 사용량이 로그되는 임계값을 지정합니다.
Process memory usage percentage to issue log info	임의 개별 프로세스의 메모리 사용량이 로그되는 임계값을 지정합니다.
Process to check, comma separated name list allowing wild cards and exclusion	검토할 하나 이상의 프로세스 이름과 일치하는 쉼표로 구분된 쿼리 목록을 지정합니다. 각 쿼리 내 와일드 카드를 사용하여 목록을 필터링할 수 있습니다. <ul style="list-style-type: none"> ■ 별표(*)는 0개 이상의 문자와 일치합니다. ■ 물음표(?)는 정확히 하나의 문자와 일치합니다. ■ 쿼리 시작 부분의 느낌표(!)는 해당 쿼리에 의해 생성된 결과를 제외시킵니다. 예를 들어, 다음 쿼리는 ws 로 시작하는 모든 프로세스를 선택하고 sys 로 끝나는 모든 프로세스를 제외시킵니다. ' !*sys,ws* '

참고 성능 알람 설정은 Horizon 연결 서버 및 Horizon Agent 시스템에만 적용됩니다. Horizon Client 시스템에는 적용되지 않습니다.

보안 설정

[표 7-6](#)에는 Horizon 일반 구성 ADMX 템플릿 파일의 보안 설정에 대해 설명되어 있습니다. 모든 설정은 그룹 정책 관리 편집기의 **컴퓨터 구성 > 정책 > 관리 템플릿 > VMware View 일반 구성 > 보안 설정** 폴더에 있습니다.

표 7-6. View 일반 구성 템플릿: 보안 설정

설정	속성
Only use cached revocation URLs	인증서 해지 검사는 캐시된 URL에만 액세스합니다. 구성되어 있지 않은 경우 기본값은 false입니다.
Revocation URL check timeout milliseconds	모든 해지 URL 연결 검색에서의 누적 시간 초과(밀리초)입니다. 구성되어 있지 않거나 0으로 설정된 값은 Microsoft 기본 처리가 사용됨을 의미합니다.
Type of certificate revocation check	완료할 인증서 해지 검사 유형을 선택합니다. <ul style="list-style-type: none"> ■ 없음 ■ EndCertificateOnly ■ WholeChain ■ WholeChain 기본값은 WholeChainButRoot입니다.

일반 설정

[표 7-7](#)에는 Horizon 일반 구성 ADMX 템플릿 파일의 일반 설정에 대해 설명되어 있습니다. 모든 설정은 그룹 정책 관리 편집기의 **컴퓨터 구성 > 정책 > 관리 템플릿 > VMware View 일반 구성** 폴더에 있습니다.

표 7-7. View 일반 구성 템플릿: 일반 설정

설정	속성
Disk threshold for log and events in Megabytes	로그 및 이벤트를 위한 최소의 남은 디스크 공간 임계값을 지정합니다. 지정된 값이 없는 경우 기본값은 200입니다. 지정된 값에 도달하면 이벤트 로깅이 중지됩니다.
Enable extended logging	추적 및 디버그 이벤트가 로그 파일에 포함되었는지 확인합니다.
Override the default View Windows event generation	지원되는 값은 다음과 같습니다. <ul style="list-style-type: none"> ■ 0 = View 이벤트에 대해서만 이벤트 로그 항목이 생성됩니다(로그 메시지에 대한 이벤트 로그 항목은 생성되지 않음). ■ 1 = 이벤트 로그 항목이 4.5 이하 호환성 모드에서 생성됩니다. 이벤트 로그 항목이 표준 View 이벤트에 대해 생성되지 않습니다. 이벤트 로그 항목이 로그 파일 텍스트만 기준으로 합니다. ■ 2 = 이벤트 로그 항목이 View 이벤트도 포함하여 4.5 이하 호환성 모드에서 생성됩니다.

Horizon 7 구성 요소 유지 보수

Horizon 7 구성 요소를 계속해서 사용하고 실행하려면 다양한 유지 관리 작업을 수행해야 합니다.

본 장은 다음 항목을 포함합니다.

- Horizon 7 구성 데이터 백업 및 복원
- Horizon 7 구성 요소 모니터링
- 시스템 상태 모니터링
- Horizon 7 서비스 이해
- 제품 라이선스 키 변경
- 제품 라이선스 사용량 모니터링
- Active Directory에서 일반 사용자 정보 업데이트
- 다른 시스템으로 View Composer 마이그레이션
- 연결 서버 인스턴스, 보안 서버 또는 View Composer의 인증서 업데이트
- 고객 환경 향상 프로그램

Horizon 7 구성 데이터 백업 및 복원

Horizon Administrator에서 자동 백업을 예약하거나 실행해 Horizon 7 및 View Composer 구성 데이터를 백업할 수 있습니다. 백업된 View LDAP 파일 및 View Composer 데이터베이스 파일을 수동으로 가져와 Horizon 7 구성을 복원할 수 있습니다.

백업 및 복원 기능을 사용해 Horizon 7 구성 데이터를 보존하고 마이그레이션할 수 있습니다.

Horizon 연결 서버 및 View Composer 데이터 백업

연결 서버의 초기 구성을 완료한 후에는 Horizon 7 및 View Composer 구성 데이터의 정기적인 백업을 스케줄링해야 합니다. Horizon 7 및 View Composer 데이터는 Horizon Administrator를 사용하여 보존할 수 있습니다.

Horizon 7은 View LDAP 저장소에 연결 서버 구성 데이터를 저장합니다. View Composer는 View Composer 데이터베이스에 연결된 클론 데스크톱 구성 데이터를 저장합니다.

Horizon Administrator를 사용하여 백업을 수행하면 Horizon 7이 View LDAP 구성 데이터와 View Composer 데이터베이스를 백업합니다. 두 백업 파일 집합은 동일한 위치에 저장됩니다. 암호화된 LDIF(LDAP 데이터 교환 형식)로 View LDAP 데이터를 내보냅니다. View LDAP에 대한 설명은 [View LDAP 디렉토리](#)에 나와 있습니다.

여러 가지 방법으로 백업 작업을 수행할 수 있습니다.

- Horizon 7 구성 백업 기능을 사용하여 자동 백업을 스케줄링하십시오.
- Horizon Administrator의 **지금 백업** 기능을 사용해 즉시 백업을 시작하십시오.
- vdmexport 유틸리티를 사용해 View LDAP 데이터를 수동으로 내보내십시오. 이 유틸리티는 연결 서버의 각 인스턴스와 함께 제공됩니다.

vdmexport 유틸리티는 View LDAP 데이터를 암호화된 LDIF 데이터, 일반 텍스트 또는 암호 및 기타 민감한 데이터가 제거된 일반 텍스트로 내보낼 수 있습니다.

참고 vdmexport 도구는 View LDAP 데이터만 백업합니다. 이 도구는 View Composer 데이터베이스 정보를 백업하지 않습니다.

vdmexport에 대한 자세한 내용은 [Horizon 연결 서버에서 구성 데이터 내보내기](#)의 내용을 참조하십시오.

다음 지침은 Horizon 7 구성 데이터 백업에 적용됩니다.

- Horizon 7은 모든 연결 서버 인스턴스에서 구성 데이터를 내보낼 수 있습니다.
- 복제된 그룹에 연결 서버 인스턴스가 여러 개 있는 경우에는 하나의 인스턴스에서만 데이터를 내보내면 됩니다. 모든 복제된 인스턴스는 동일한 구성 데이터를 포함하고 있습니다.
- 연결 서버의 복제된 인스턴스를 백업 메커니즘으로 사용하지 마십시오. Horizon 7이 연결 서버의 복제된 인스턴스에 있는 데이터를 동기화하는 경우 하나의 인스턴스에서 손실된 데이터가 그룹의 모든 구성원에서 손실될 수 있습니다.
- 연결 서버가 여러 개의 vCenter Server 인스턴스에서 여러 개의 Composer 서비스를 사용하는 경우 Horizon 7은 vCenter Server 인스턴스와 연결된 모든 View Composer 데이터베이스를 백업합니다.

Horizon 7 구성 백업 예약

Horizon 7 구성 데이터의 정기적인 백업을 예약할 수 있습니다. Horizon 7은 연결 서버 인스턴스가 구성 데이터를 저장하는 View LDAP 저장소의 콘텐츠를 백업합니다.

연결 서버 인스턴스를 선택하고 **지금 백업**을 클릭하여 구성을 즉시 백업할 수 있습니다.

사전 요구 사항

백업 설정을 숙지하십시오. [Horizon 7 구성 백업 설정](#)의 내용을 참조하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 **연결 서버** 탭에서 백업할 연결 서버 인스턴스를 선택하고 **편집**을 클릭합니다.

- 3 **백업** 탭에서 Horizon 7 구성 백업 설정을 지정하여 백업 주기, 최대 백업 수 및 백업 파일의 폴더 위치를 구성합니다.
- 4 (선택 사항) 데이터 복구 암호를 변경합니다.
 - a **데이터 복구 암호 변경**을 클릭합니다.
 - b 새 암호를 입력하고 확인합니다.
 - c (선택 사항) 암호 알림을 입력합니다.
 - d **확인**을 클릭합니다.
- 5 **확인**을 클릭합니다.

Horizon 7 구성 백업 설정

Horizon 7은 정기적으로 연결 서버 및 View Composer 구성 데이터를 백업할 수 있습니다. Horizon Administrator에서 백업 작업의 빈도 및 다른 측면을 설정할 수 있습니다.

표 8-1. Horizon 7 구성 백업 설정

설정	설명
자동 백업 빈도	<p>1시간마다. 백업이 1시간마다 발생합니다.</p> <p>6시간마다. 백업이 자정, 오전 6시, 정오 및 오후 6시에 발생합니다.</p> <p>12시간마다. 백업이 자정 및 정오에 발생합니다.</p> <p>매일. 백업이 매일 자정에 발생합니다.</p> <p>2일마다. 백업이 토요일, 월요일, 수요일, 금요일 자정에 발생합니다.</p> <p>매주. 백업이 매주 토요일 자정에 발생합니다.</p> <p>2주마다. 백업이 격주로 토요일 자정에 발생합니다.</p> <p>안 함. 백업이 자동으로 발생하지 않습니다.</p>
최대 백업 수	<p>연결 서버 인스턴스에 저장될 수 있는 백업 파일의 수. 백업 파일 수는 0보다 큰 정수여야 합니다.</p> <p>최대값에 도달할 경우 Horizon 7이 가장 오래된 백업 파일을 삭제합니다.</p> <p>또한 이 설정은 지금 백업을 사용할 때 생성된 백업 파일에 적용됩니다.</p>
폴더 위치	<p>연결 서버가 실행되고 있는 컴퓨터의 백업 파일 기본 위치:</p> <p>C:\Programdata\VMware\WVDM\backups</p> <p>지금 백업을 사용할 경우 Horizon 7 또한 이 위치에 백업 파일을 저장합니다.</p>

Horizon 연결 서버에서 구성 데이터 내보내기

View LDAP 저장소에서 Horizon 연결 서버 인스턴스의 구성 데이터 내용을 내보내서 백업할 수 있습니다.

암호화된 LDIF 파일로 View LDAP 구성 데이터를 내보내려면 `vdmexport` 명령을 사용하십시오. `vdmexport -v`(약어) 옵션을 사용해 일반 텍스트 LDIF 파일로 데이터를 내보내거나 `vdmexport -c`(정리됨) 옵션을 사용해 암호 및 기타 민감한 데이터가 제거된 일반 텍스트로 데이터를 내보낼 수도 있습니다.

모든 연결 서버 인스턴스에서 `vdmexport` 명령을 실행할 수 있습니다. 복제된 그룹에 연결 서버 인스턴스가 여러 개 있는 경우에는 하나의 인스턴스에서만 데이터를 내보내면 됩니다. 모든 복제된 인스턴스는 동일한 구성 데이터를 포함하고 있습니다.

참고 `vdmexport` 명령은 View LDAP 데이터만 백업합니다. 이 명령으로 View Composer 데이터베이스 정보를 백업할 수 없습니다.

사전 요구 사항

- 기본 경로에서 연결 서버와 함께 설치된 명령 실행 파일 `vdmexport.exe`를 찾으십시오.
C:\Program Files\VMware\VMware View\Server\tools\bin
- 관리자 또는 관리자(읽기 전용) 역할에서 사용자로 연결 서버 인스턴스에 로그인하십시오.

절차

- 1 시작 > 명령 프롬프트를 선택합니다.
- 2 명령 프롬프트에 `vdmexport` 명령을 입력하고 파일로 출력을 리디렉션하십시오. 예:

```
vdmexport > Myexport.LDF
```

기본적으로 내보낸 데이터는 암호화됩니다.

출력 파일 이름을 `-f` 옵션에 대한 인수로 지정할 수 있습니다. 예:

```
vdmexport -f Myexport.LDF
```

`-v` 옵션을 사용해 일반 텍스트 형식(약어)으로 데이터를 내보낼 수 있습니다. 예:

```
vdmexport -f Myexport.LDF -v
```

`-c` 옵션을 사용해 암호 및 기타 민감한 데이터가 제거된(정리됨) 일반 텍스트 형식으로 데이터를 내보낼 수 있습니다. 예:

```
vdmexport -f Myexport.LDF -c
```

참고 정리된 백업 데이터를 사용해 View LDAP 구성을 복원하지 마십시오. 정리된 구성 데이터에는 암호와 기타 중요 정보가 누락되어 있습니다.

`vdmexport` 명령에 대한 자세한 내용은 Horizon 7 통합 문서를 참조하십시오.

다음에 수행할 작업

`vdmimport` 명령을 사용해 연결 서버의 구성 정보를 복원하거나 전송할 수 있습니다.

LDIF 파일 내보내기에 대한 자세한 내용은 [Horizon 연결 서버 및 View Composer 구성 데이터 복원](#)에 나와 있습니다.

Horizon 연결 서버 및 View Composer 구성 데이터 복원

Horizon 7에서 백업한 View Composer 데이터베이스 파일 및 연결 서버 LDAP 구성 파일을 수동으로 복원할 수 있습니다.

개별 유틸리티를 수동으로 실행하여 연결 서버 및 View Composer 구성 데이터를 복원합니다.

구성 데이터를 복원하기 전에 Horizon Administrator의 구성 데이터를 백업했는지 확인합니다.

[Horizon 연결 서버 및 View Composer 데이터 백업](#)의 내용을 참조하십시오.

vdmimport 유틸리티를 사용하여 LDIF 백업 파일의 연결 서버 데이터를 연결 서버 인스턴스의 View LDAP 저장소로 가져옵니다.

SviConfig 유틸리티를 사용하여 .svi 백업 파일의 View Composer 데이터를 View Composer SQL 데이터베이스로 가져올 수 있습니다.

참고 경우에 따라서는 현재 버전의 연결 서버 인스턴스를 설치하고 연결 서버 LDAP 구성 파일을 가져와 기존 Horizon 7 구성을 복원해야 할 수 있습니다. 이 절차는 비즈니스 연속성 및 재난 복구 (BC/DR) 계획의 일부로 기존 Horizon 7 구성을 사용하여 두 번째 데이터 센터를 설정하는 단계 또는 기타 이유로 필요할 수 있습니다. 자세한 내용은 Horizon 7 설치 문서를 참조하십시오.

Horizon 연결 서버로 구성 데이터 가져오기

LDIF 파일에 저장되어 있는 데이터 백업 복사본을 가져와 연결 서버 인스턴스의 데이터 구성을 복원할 수 있습니다.

vdmimport 명령을 사용해 LDIF 파일에서 연결 서버 인스턴스의 LDAP 저장소로 데이터를 가져옵니다.

Horizon Administrator 또는 기본 vdmexport 명령을 사용해 View LDAP 구성을 백업한 경우 내보낸 LDIF 파일이 암호화됩니다. LDIF 파일을 암호화해야만 가져올 수 있습니다.

내보낸 LDIF 파일의 형식이 일반 텍스트인 경우 파일을 암호화하지 않아도 됩니다.

참고 암호와 기타 민감한 데이터가 정리된 일반 텍스트인 정리된 형식으로 LDIF 파일을 가져오지 마십시오. 그렇지 않으면 복원된 View LDAP 저장소에서 중요 구성 정보가 누락됩니다.

View LDAP 저장소 백업에 대한 자세한 내용은 [Horizon 연결 서버 및 View Composer 데이터 백업](#)에 나와 있습니다.

사전 요구 사항

- 기본 경로에서 연결 서버와 함께 설치된 명령 실행 파일 vdmimport를 찾으십시오.
C:\Program Files\VMware\VMware View\Server\tools\bin
- 관리자 역할의 사용자로 연결 서버 인스턴스에 로그인하십시오.
- 데이터 복구 암호를 알고 있는지 확인하십시오. 암호 알림이 구성된 경우 암호 옵션 없이 vdmimport 명령을 실행하여 알림을 표시할 수 있습니다.

절차

- 1 View Composer가 실행되는 서버에서 Windows 서비스 VMware Horizon View Composer를 중지하여 모든 View Composer 인스턴스를 중지합니다.
- 2 모든 보안 서버에서 Windows 서비스 VMware Horizon 보안 서버를 중지하여 모든 보안 서버 인스턴스를 중지합니다.
- 3 모든 Horizon 연결 서버 인스턴스를 제거합니다.
VMware Horizon 연결 서버와 AD LDS 인스턴스 VMwareVDMDS를 모두 제거합니다.
- 4 연결 서버 인스턴스를 하나 설치합니다.
- 5 Windows 서비스 VMware Horizon 연결 서버를 중지하여 연결 서버 인스턴스를 중지합니다.
- 6 **시작 > 명령 프롬프트**를 클릭합니다.
- 7 암호화된 LDIF 파일의 암호를 해독합니다.

명령 프롬프트에 vdmimport 명령을 입력합니다. -d 옵션, 데이터 복구 암호를 포함한 -p 옵션, 기존의 암호화된 LDIF 파일 뒤에 암호가 해독된 LDIF 파일의 이름이 오는 -f 옵션을 지정합니다. 예:

```
vdmimport -d -p mypassword
-f MyEncryptedexport.LDF > MyDecryptedexport.LDF
```

데이터 복구 암호가 기억나지 않으면 -p 옵션 없이 명령을 입력하십시오. 유틸리티에 암호 알림이 표시되고 암호를 입력하라는 메시지가 나타납니다.

- 8 암호화된 LDIF 파일을 가져와 View LDAP 구성을 복원합니다.

암호가 해독된 LDIF 파일을 포함한 -f 옵션을 지정합니다. 예:

```
vdmimport -f MyDecryptedexport.LDF
```

- 9 연결 서버를 제거합니다.
VMware Horizon 연결 서버 패키지만 제거합니다.
- 10 연결 서버를 재설치합니다.
- 11 Horizon Administrator에 로그인하여 구성이 올바른지 확인합니다.
- 12 View Composer 인스턴스를 시작합니다.
- 13 복제 서버 인스턴스를 재설치합니다.
- 14 보안 서버 인스턴스를 시작합니다.

또한 보안 서버의 구성이 일치하지 않을 위험이 있으면 중지하는 대신 제거했다가 프로세스가 끝날 때 재설치해야 합니다.

vdmimport는 LDIF 파일의 구성 데이터를 사용해 연결 서버의 View LDAP 저장소를 업데이트하는 명령입니다. vdmimport 명령에 대한 자세한 내용은 Horizon 7 설치 문서를 참조하십시오.

참고 복원 중인 구성이 vCenter Server 및 View Composer(사용 중인 경우)에 알려진 가상 시스템과 일치하는지 확인하십시오. 필요한 경우 백업에서 View Composer 구성을 복원하십시오. [View Composer 데이터베이스 복원](#)의 내용을 참조하십시오. View Composer 구성 백업 이후 vCenter Server의 가상 시스템이 변경된 경우에는 View Composer 구성을 복원한 후 불일치를 수동으로 해결해야 할 수 있습니다.

View Composer 데이터베이스 복원

View Composer 구성의 백업 파일을 연결된 클론 정보가 저장된 View Composer 데이터베이스로 가져올 수 있습니다.

SviConfig restoredata 명령을 사용하여 시스템 실패 후 View Composer 데이터베이스 데이터를 복원하거나 View Composer 구성을 이전 상태로 복구할 수 있습니다.

중요 경험 있는 View Composer 관리자만 SviConfig 유틸리티를 사용해야 합니다. 이 유틸리티는 View Composer 서비스와 관련된 문제를 해결하기 위해 제작되었습니다.

사전 요구 사항

View Composer 데이터베이스 백업 파일의 위치를 확인하십시오. 기본적으로 Horizon 7은 연결 서버 컴퓨터의 C: 드라이브(C:\ProgramData\VMware\WDM\backups)에 백업 파일을 저장합니다.

View Composer 백업 파일은 날짜 스탬프 및 .svi 접미사를 가진 이름 지정 규칙을 사용합니다.

Backup-YearMonthDayCount-vCenter Server Name_Domain Name.svi

예: Backup-20090304000010-foobar_test_org.svi

SviConfig restoredata 매개 변수를 숙지하십시오.

- DsnName - 데이터베이스에 연결하는 데 사용되는 DSN입니다. DsnName 매개 변수는 필수 항목이며 빈 문자열일 수 없습니다.
- Username - 데이터베이스에 연결하는 데 사용되는 사용자 이름입니다. 이 매개 변수가 지정되지 않은 경우 Windows 인증이 사용됩니다.
- Password - 데이터베이스에 연결하는 데 사용되는 사용자 암호입니다. 이 매개 변수가 지정되지 않은 경우 Windows 인증이 사용되지 않고 나중에 암호를 입력하라는 메시지가 나타납니다.
- BackupFilePath - View Composer 백업 파일의 경로입니다.

DsnName 및 BackupFilePath 매개 변수는 필수 매개 변수이며 빈 문자열일 수 없습니다. Username 및 Password 매개 변수는 선택 사항입니다.

절차

- 1 연결 서버 컴퓨터의 View Composer 백업 파일을 VMware Horizon View Composer 서비스가 설치된 컴퓨터에서 액세스할 수 있는 위치에 복사합니다.

- 2 View Composer가 설치된 컴퓨터에서 VMware Horizon View Composer 서비스를 중지합니다.
- 3 Windows 명령 프롬프트를 열고 SviConfig 실행 파일로 이동합니다.

파일은 View Composer 애플리케이션으로 찾을 수 있습니다. 기본 경로는 C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe입니다.

- 4 SviConfig restoredata 명령을 실행하십시오.

```
sviconfig -operation=restoredata
          -DsnName=target_database_source_name_(DSN)
          -Username=database_administrator_username
          -Password=database_administrator_password
          -BackupFilePath=path_to_View_Composer_backup_file
```

예 :

```
sviconfig -operation=restoredata -dsnname=LinkedClone
          -username=Admin -password=Pass
          -backupfilepath="C:\Program Files (x86)\VMware\VMware View
          Composer\Backup-20090304000010-foobar_test_org.SVI"
```

- 5 VMware Horizon View Composer 서비스를 시작합니다.

다음에 수행할 작업

SviConfig restoredata 명령의 출력 결과 코드는 [View Composer 데이터베이스 복원 결과 코드](#)의 내용을 참조하십시오.

View Composer 데이터베이스 복원 결과 코드

View Composer 데이터베이스를 복원할 경우 SviConfig restoredata 명령이 결과 코드를 표시합니다.

표 8-2. Restoredata 결과 코드

코드	설명
0	작업을 성공적으로 마쳤습니다.
1	제공된 DSN을 찾을 수 없습니다.
2	잘못된 데이터베이스 관리자 자격 증명이 제공되었습니다.
3	데이터베이스의 드라이버가 지원되지 않습니다.
4	예기치 않은 문제가 발생했고 명령이 완료되지 못했습니다.
14	다른 애플리케이션이 VMware Horizon View Composer 서비스를 사용 중입니다. 명령을 실행하기 전에 서비스를 종료하십시오.
15	복원 프로세스 중 문제가 발생했습니다. 자세한 내용은 화면 로그 출력에 제공됩니다.

View Composer 데이터베이스의 데이터 내보내기

View Composer 데이터베이스에서 파일로 데이터를 내보낼 수 있습니다.

중요 SviConfig 유틸리티는 경험 많은 View Composer 관리자인 경우에만 사용하십시오.

사전 요구 사항

기본적으로 Horizon 7는 C: 드라이브(C:\Programdata\VMware\VMware\backups)에 백업 파일을 저장합니다.

SviConfig exportdata 매개 변수를 숙지하십시오.

- DsnName - 데이터베이스에 연결하는 데 사용되는 DSN입니다. 지정되지 않은 경우 서버 구성 파일에서 DSN 이름, 사용자 이름 및 암호가 검색됩니다.
- Username - 데이터베이스에 연결하는 데 사용되는 사용자 이름입니다. 이 매개 변수가 지정되지 않은 경우 Windows 인증이 사용됩니다.
- Password - 데이터베이스에 연결하는 데 사용되는 사용자 암호입니다. 이 매개 변수가 지정되지 않은 경우 Windows 인증이 사용되지 않고 나중에 암호를 입력하라는 메시지가 나타납니다.
- OutputFilePath - 출력 파일의 경로입니다.

절차

- 1 View Composer가 설치된 컴퓨터에서 VMware Horizon View Composer 서비스를 중지합니다.

- 2 Windows 명령 프롬프트를 열고 SviConfig 실행 파일로 이동합니다.

파일은 View Composer 애플리케이션으로 찾을 수 있습니다.

View-Composer-installation-directory\sviconfig.exe

- 3 SviConfig exportdata 명령을 실행합니다.

```
sviconfig -operation=exportdata
          -DsnName=target_database_source_name_(DSN)
          -Username=database_administrator_username
          -Password=database_administrator_password
          -OutputFilePath=path_to_View_Composer_output_file
```

예 :

```
sviconfig -operation=exportdata -dsname=LinkedClone
          -username=Admin -password=Pass
          -outputfilepath="C:\Program Files\VMware\VMware View
          Composer\Export-20090304000010-foobar_test_org.SVI"
```


다음에 수행할 작업

SviConfig exportdata 명령의 내보내기 결과 코드는 [View Composer 데이터베이스 내보내기 결과 코드](#)의 내용을 참조하십시오.

View Composer 데이터베이스 내보내기 결과 코드

View Composer 데이터베이스를 내보낼 경우 SviConfig exportdata 명령이 종료 코드를 표시합니다.

표 8-3. Exportdata ExitStatus 코드

코드	설명
0	데이터 내보내기가 성공적으로 끝났습니다.
1	지정된 DSN 이름을 찾을 수 없습니다.
2	지정된 자격 증명이 잘못되었습니다.
3	제공된 데이터베이스에는 지원되지 않는 드라이버입니다.
4	예기치 않은 문제가 발생했습니다.
18	데이터베이스 서버에 연결할 수 없습니다.
24	출력 파일을 열 수 없습니다.

Horizon 7 구성 요소 모니터링

Horizon Administrator 대시보드를 사용해 Horizon 7 배포에서 Horizon 7 및 vSphere 구성 요소의 상태를 신속하게 조사할 수 있습니다.

Horizon Administrator는 연결 서버 인스턴스, 이벤트 데이터베이스, 게이트웨이, 보안 서버, View Composer 서비스, 데이터스토어, vCenter Server 인스턴스 및 도메인에 대한 모니터링 정보를 표시합니다.

참고 Horizon 7는 Kerberos 도메인에 대한 상태 정보를 확인할 수 없습니다. Horizon Administrator는 도메인이 구성되고 작동하는 상태에서도 Kerberos 도메인 상태를 알 수 없음으로 표시합니다.

절차

- 1 Horizon Administrator에서 **대시보드**를 클릭합니다.
- 2 시스템 상태 창에서 **View 구성 요소**, **vSphere 구성 요소** 또는 **기타 구성 요소**를 확장하십시오.
 - 녹색 위쪽 화살표는 구성 요소에 문제가 없음을 나타냅니다.
 - 빨간색 아래쪽 화살표는 구성 요소를 사용할 수 없거나 작동하지 않음을 나타냅니다.
 - 노란색 양방향 화살표는 구성 요소가 경고 상태에 있음을 나타냅니다.
 - 물음표는 구성 요소 상태를 알 수 없음을 나타냅니다.

- 3 구성 요소 이름을 클릭합니다.

대화 상자에 이름, 버전, 상태 및 기타 구성 요소 정보가 표시됩니다.

다음에 수행할 작업

vCenter Server를 사용하여 vSAN 클러스터 및 vSAN 데이터스토어에 속한 모든 디스크를 모니터링합니다. vSphere 5.5 업데이트 1의 vSAN 모니터링에 대한 자세한 내용은 vSphere 스토리지 문서와 vSphere 모니터링 및 성능 설명서를 참조하십시오. vSphere 6 이상의 vSAN 모니터링에 대한 자세한 내용은 VMware vSAN 관리 문서를 참조하십시오.

시스템 상태 모니터링

Horizon Administrator 대시보드를 사용하여 Horizon 7 배포에서 시스템의 상태를 신속하게 조사할 수 있습니다. 예를 들어, 연결이 끊어진 모든 시스템 또는 유지 관리 모드에 있는 시스템을 표시할 수 있습니다.

사전 요구 사항

가상 시스템 상태 값을 숙지하십시오. 가상 시스템 상태에 대한 자세한 내용은 Horizon 7에서 가상 데스크톱 설정 문서의 "vCenter Server 가상 시스템 상태"를 참조하십시오.

절차

- 1 Horizon Administrator에서 **대시보드**를 클릭합니다.
- 2 시스템 상태 창에서 상태 폴더를 확장합니다.

옵션	설명
준비 중	시스템이 프로비저닝 또는 삭제 중이거나 유지 관리 모드에 있는 동안의 상태를 나열합니다.
문제가 있는 시스템	오류 상태를 나열합니다.
사용할 준비가 됨	시스템을 사용할 준비가 되었을 때의 상태를 나열합니다.

- 3 시스템 상태를 찾고 상태 옆에 있는 하이퍼링크된 숫자를 클릭합니다.

선택한 상태에 있는 모든 시스템이 **시스템** 페이지에 표시됩니다.

다음에 수행할 작업

시스템 이름을 클릭하여 시스템에 대한 세부 정보를 보거나 Horizon Administrator에서 뒤로 화살표를 클릭하여 대시보드 페이지로 돌아갈 수 있습니다.

Horizon 7 서비스 이해

연결 서버 인스턴스 및 보안 서버의 작업은 시스템에서 실행되는 여러 서비스에 따라 다릅니다. 이러한 시스템은 자동으로 시작 및 중지되지만 때때로 이러한 서비스 작업을 수동으로 조정해야 할 수도 있습니다.

Microsoft Windows 서비스 도구를 사용하여 Horizon 7 서비스를 중지하거나 시작할 수 있습니다. 연결 서버 호스트 또는 보안 서버에서 Horizon 7을 중지할 경우, 서비스를 다시 시작할 때까지 최종 사용자가 원격 데스크톱이나 애플리케이션에 연결할 수 없습니다. 또한 서비스 실행이 중지되었거나, 서비스가 제어하는 Horizon 7 기능이 응답하지 않는 경우에는 서비스를 다시 시작해야 할 수도 있습니다.

Horizon 7 서비스 중지 및 시작

연결 서버 인스턴스 및 보안 서버의 작업은 시스템에서 실행되는 여러 서비스에 따라 다릅니다. 때때로 Horizon 7의 작업 문제를 해결할 때 이러한 서비스를 수동으로 중지 및 시작해야 할 수 있습니다.

Horizon 7 서비스를 중지하면 최종 사용자가 원격 데스크톱과 애플리케이션에 연결할 수 없습니다. 시스템 유지 관리를 위해 이미 예약된 시간에 해당 작업을 수행하거나 최종 사용자에게 일시적으로 데스크톱과 애플리케이션을 사용할 수 없게 된다고 경고해야 합니다.

참고 연결 서버 호스트의 VMware Horizon View 연결 서버 서비스 또는 보안 서버의 VMware Horizon View 보안 서버 서비스만 중지하십시오. 다른 구성 요소 서비스는 중지하지 마십시오.

사전 요구 사항

연결 서버 호스트의 서비스 및 보안 서버의 서비스에 설명된 대로 연결 서버 호스트 및 보안 서버에서 실행되는 서비스를 숙지하십시오.

절차

- 1 명령 프롬프트에 **services.msc**를 입력하여 Windows Services 도구를 시작하십시오.
- 2 연결 서버 호스트의 VMware Horizon View 연결 서버 서비스 또는 보안 서버의 VMware Horizon View 보안 서버 서비스를 선택하고, 적절한 경우 **중지**, **다시 시작** 또는 **시작**을 클릭합니다.
- 3 예상대로 나열된 서비스의 상태가 변경되는지 확인합니다.

연결 서버 호스트의 서비스

Horizon 7의 작업은 연결 서버 호스트에서 실행할 여러 서비스에 따라 달라집니다.

표 8-4. Horizon 연결 서버 호스트 서비스

서비스 이름	시작 유형	설명
VMware Horizon View Blast 보안 게이트웨이	자동	보안 HTML Access 및 Blast Extreme 서비스를 제공합니다. 이 서비스는 클라이언트가 Blast 보안 게이트웨이를 통해 연결 서버에 연결할 경우 실행 중이어야 합니다.
VMware Horizon View 연결 서버	자동	연결 브로커 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다. 이 서비스를 시작 또는 중지할 경우 Framework, Message Bus, Security Gateway 및 Web 서비스 또한 시작 또는 중지합니다. 이 서비스는 VMwareVDMDS 또는 VMware Horizon View Script Host 서비스를 시작 또는 중지하지 않습니다.
VMware Horizon View Framework 구성 요소	수동	이벤트 로깅, 보안 및 COM+ 프레임워크 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다.
VMware Horizon View Message Bus 구성 요소	수동	Horizon 7 구성 요소 간 메시징 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다.

표 8-4. Horizon 연결 서버 호스트 서비스 (계속)

서비스 이름	시작 유형	설명
VMware Horizon View PCoIP 보안 게이트웨이	수동	PCoIP Secure Gateway 서비스를 제공합니다. 이 서비스는 클라이언트가 PCoIP 보안 게이트웨이를 통해 연결 서버에 연결할 경우 실행 중이어야 합니다.
VMware Horizon View Script Host	사용 안 함	가상 시스템을 삭제할 때 실행된 타사 스크립트의 지원을 제공합니다. 이 서비스가 기본적으로 사용되지 않도록 설정됩니다. 스크립트를 실행할 경우 이 서비스를 사용하도록 설정해야 합니다.
VMware Horizon View Security Gateway 구성 요소	수동	공용 게이트웨이 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다.
VMware Horizon View 웹 구성 요소	수동	웹 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다.
VMwareVDMDS	자동	LDAP 디렉터리 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다. Horizon 7을 업그레이드하는 동안 이 서비스는 기존 데이터가 올바르게 마이그레이션 되도록 합니다.

보안 서버의 서비스

Horizon 7의 작업은 보안 서버에서 실행되는 몇 가지 서비스에 따라 달라집니다.

표 8-5. 보안 서버 서비스

서비스 이름	시작 유형	설명
VMware Horizon View Blast 보안 게이트웨이	자동	보안 HTML Access 및 Blast Extreme 서비스를 제공합니다. 클라이언트가 Blast 보안 게이트웨이를 통해 이 보안 서버에 연결하는 경우에는 이 서비스가 반드시 실행되어야 합니다.
VMware Horizon View 보안 서버	자동	보안 서버 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다. 이 서비스를 시작 또는 중지할 경우 Framework 및 Security Gateway 서비스 또한 시작 또는 중지합니다.
VMware Horizon View Framework 구성 요소	수동	이벤트 로깅, 보안 및 COM+ 프레임워크 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다.
VMware Horizon View PCoIP 보안 게이트웨이	수동	PCoIP Secure Gateway 서비스를 제공합니다. 클라이언트가 PCoIP 보안 게이트웨이를 통해 이 보안 서버에 연결하는 경우에는 이 서비스가 반드시 실행되어야 합니다.
VMware Horizon View Security Gateway 구성 요소	수동	공용 게이트웨이 서비스를 제공합니다. 이 서비스는 항상 실행되어야 합니다.

제품 라이선스 키 변경

현재 시스템에서 라이선스가 만료되었거나, 라이선스가 없는 Horizon 7 기능에 액세스하려는 경우에는 Horizon Administrator를 사용하여 제품 라이선스 키를 변경할 수 있습니다.

Horizon 7가 실행 중인 동안 Horizon 7에 라이선스를 추가할 수 있습니다. 시스템을 다시 부팅할 필요가 없으며 데스크톱 및 애플리케이션 액세스가 중단되지 않습니다.

사전 요구 사항

Horizon 7를 비롯하여 View Composer와 게시된 애플리케이션 같은 추가 기능이 제대로 작동하게 하려면 유효한 제품 라이선스 키를 구입하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 제품 라이선싱 및 사용량**을 선택합니다.

현재 라이선스 키의 처음과 마지막 다섯 자가 **라이선싱** 패널에 표시됩니다.

- 2 **라이선스 편집**을 클릭합니다.

- 3 라이선스 일련 번호를 입력하고 **확인**을 클릭합니다.

제품 라이선싱 창에 업데이트된 라이선싱 정보가 표시됩니다.

- 4 라이선스 만료 날짜를 확인하십시오.

- 5 제품 라이선스에서 사용 권한을 부여하는 VMware Horizon 7을 기준으로 데스크톱 라이선스, 애플리케이션 원격 라이선스 및 View Composer 라이선스가 사용되도록 설정되었는지 또는 사용되지 않도록 설정되었는지 확인합니다.

VMware Horizon 7의 일부 특징과 기능은 버전에 따라 제공되지 않을 수 있습니다. 버전별 기능 세트 비교는

<http://www.vmware.com/files/pdf/products/horizon-view/VMware-Horizon-View-Pricing-Licensing-FAQ.pdf>를 참조하십시오.

- 6 라이선싱 사용량 모델이 제품 라이선스에 사용된 모델과 일치하는지 확인합니다.

사용량은 제품 라이선스의 버전과 사용량 계약에 따라 명명된 사용자 또는 동시 사용자 수를 기준으로 계산됩니다.

제품 라이선스 사용량 모니터링

Horizon 7 Administrator에서 Horizon에 동시 연결된 활성 사용자를 모니터링할 수 있습니다. **제품 라이선싱 및 사용량** 페이지에는 현재 및 가장 높은 기록 사용량 수가 표시됩니다. 이러한 숫자를 사용하여 제품 라이선스 사용량을 추적할 수 있습니다. 기록 사용량 데이터를 재설정하고 현재 데이터로 다시 시작할 수도 있습니다.

Horizon에서는 두 개의 라이선싱 사용량 모델을 제공하며, 하나는 명명된 사용자에게 사용되고 하나는 동시 사용자에게 사용됩니다. Horizon에서는 제품 라이선스 버전이나 사용량 모델 계약에 관계없이 환경에 있는 명명된 사용자와 동시 사용자 수를 계산합니다.

명명된 사용자의 경우, Horizon에서는 Horizon 환경에 액세스한 고유 사용자의 수를 계산합니다. 명명된 사용자가 여러 개의 단일 사용자 데스크톱, 게시된 데스크톱 및 게시된 애플리케이션을 실행하는 경우 사용자는 한 번만 계산됩니다.

명명된 사용자의 경우 **제품 라이선싱 및 사용량** 페이지의 **현재** 열에는 Horizon 배포를 처음 구성하거나 **명명된 사용자 수**를 마지막으로 재설정 한 후의 사용자 수를 표시합니다. 명명된 사용자에게는 **최고** 열이 적용되지 않습니다.

동시 사용자의 경우, Horizon에서는 세션당 단일 사용자 데스크톱 연결 수를 확인합니다. 사용자가 여러 단일 사용자 데스크톱을 실행하면 연결된 데스크톱 세션이 각각 개별적으로 계산됩니다.

동시 사용자의 게시된 데스크톱 및 애플리케이션 연결은 사용자별로 계산됩니다. 동시 사용자가 여러 개의 게시된 데스크톱 세션과 애플리케이션을 실행하면 서로 다른 RDS 호스트에 서로 다른 게시된 데스크톱 및 애플리케이션을 호스팅한 경우라도 사용자가 한 번만 계산됩니다. 동시 사용자가 단일 사용자 데스크톱과 추가 게시된 데스크톱 및 애플리케이션을 실행할 경우 사용자는 한 번만 계산됩니다.

동시 사용자의 경우 **제품 라이선싱 및 사용량** 페이지의 **최고** 열에는 Horizon 배포를 처음 구성하거나 **최고 수**를 마지막으로 재설정 한 후의 동시 데스크톱 세션과 게시된 데스크톱 및 애플리케이션의 최고 사용자 수가 표시됩니다.

공동 작업 세션 및 세션에 연결된 세션 공동 작업자 수를 모니터링할 수 있습니다.

- **활성 - 공동 작업 세션:** 세션 소유자가 한 명 이상의 사용자를 세션에 가입하도록 초대한 세션 수입니다. 예: John은 세션에 가입하도록 두 명의 사람을 초대했으며 Mary는 세션에 가입하도록 한 명의 사람을 초대했습니다. 초대를 받은 사람이 세션에 가입했는지 여부에 관계없이 이 행의 값은 2입니다.
- **활성 - 총 공동 작업자:** 세션 소유자 및 공동 작업자를 포함하여 공동 작업 세션에 연결된 사용자의 총 수입니다. 예: John은 두 사람을 초대했으며 한 명만 세션에 가입했습니다. Mary는 세션에 가입하지 않은 한 사람을 초대했습니다. 이 행의 값은 3입니다. John의 공동 작업 세션에는 한 명의 기본 사용자와 한 명의 보조 사용자가 있지만 Mary의 공동 작업 세션에는 한 명의 기본 사용자가 있고 보조 사용자는 없습니다. 세션 소유자가 계산되기 때문에 공동 작업자의 총 수는 항상 공동 작업 세션의 총 수보다 크거나 같습니다.

제품 라이선스 사용량 데이터 재설정

Horizon Administrator에서 기록 제품 사용량 데이터를 재설정하고 현재 데이터로 다시 시작할 수 있습니다.

전역 구성 및 정책 관리 권한이 있는 관리자는 **최고 개수 재설정** 및 **명명된 사용자 수 재설정** 설정을 선택할 수 있습니다. 이러한 설정에 대한 액세스를 제한하려면 지정된 관리자에게만 이 권한을 제공하십시오.

사전 요구 사항

제품 라이선스 사용 방법을 숙지합니다. [제품 라이선스 사용량 모니터링](#)의 내용을 참조하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 제품 라이선싱 및 사용량**을 선택합니다.

- 2 (선택 사항) **사용량** 창에서 **최고 개수 재설정**을 선택합니다.

가장 높은 기록 동시 연결 수가 현재 동시 연결 수로 재설정됩니다.

- 3 (선택 사항) **사용량** 창에서 **명명된 사용자 수 재설정**을 선택합니다.

명명된 사용자 수 최고 기록이 0으로 재설정됩니다.

참고 사용자 및 그룹 페이지에서 **일반 사용자 정보 업데이트**를 선택해도 명명된 사용자 수 최고 기록이 0으로 재설정됩니다.

Active Directory에서 일반 사용자 정보 업데이트

Active Directory에 저장된 현재 사용자 정보로 Horizon 7를 업데이트할 수 있습니다. 이 기능은 Horizon 7 사용자의 이름, 전화, e-메일, 사용자 이름 및 기본 Windows 도메인을 업데이트합니다. 또한 신뢰된 외부 도메인이 업데이트됩니다.

Active Directory의 신뢰된 외부 도메인 목록을 수정할 경우, 특히 도메인 간 변경된 신뢰 관계가 Horizon 7의 사용자 사용 권한에 영향을 줄 경우 이 기능을 사용하십시오.

이 기능은 최신 사용자 정보에 대해 Active Directory를 스캔하고 Horizon 7 구성을 새로 고칩니다.

일반 사용자 정보를 업데이트하면 명명된 사용자의 수도 0으로 재설정됩니다. 이 값은 Horizon Administrator의 **제품 라이선싱 및 사용량** 페이지에 표시됩니다. [제품 라이선스 사용량 데이터 재설정](#)의 내용을 참조하십시오.

또한 vdmadmin 명령을 사용하여 사용자 및 도메인 정보를 업데이트할 수 있습니다. [-F 옵션을 사용하여 외부 보안 주체 업데이트](#)의 내용을 참조하십시오.

사전 요구 사항

Horizon Administrator에 **전역 구성 및 정책 관리** 권한이 있는 관리자로 로그인할 수 있는지 확인합니다.

절차

- Horizon Administrator에서 **사용자 및 그룹**을 클릭합니다.
- 모든 사용자 또는 개별 사용자의 정보를 업데이트할지 여부를 선택합니다.

옵션	조치
모든 사용자용	<p>일반 사용자 정보 업데이트를 클릭합니다.</p> <p>모든 사용자 및 그룹을 업데이트하는 데 오랜 시간이 걸릴 수 있습니다.</p>
개별 사용자용	<p>a 업데이트할 사용자 이름을 클릭합니다.</p> <p>b 일반 사용자 정보 업데이트를 클릭합니다.</p>

다른 시스템으로 View Composer 마이그레이션

새 Windows Server 가상 또는 물리적 시스템에 VMware Horizon View Composer 서비스를 마이그레이션해야 하는 경우가 있습니다. 예를 들면, View Composer 및 vCenter Server를 새 ESXi 호스트 또는 클러스터로 마이그레이션하여 Horizon 7 배포를 확장할 수 있습니다. 또한 동일한 Windows Server 시스템에 View Composer와 vCenter Server를 설치할 필요가 없습니다.

vCenter Server 시스템에서 독립 실행형 시스템으로, 또는 독립 실행형 시스템에서 vCenter Server 시스템으로 View Composer를 마이그레이션할 수 있습니다.

- **View Composer 마이그레이션 지침**

VMware Horizon View Composer 서비스를 마이그레이션할 때 수행하는 단계는 기존의 연결된 클론 가상 시스템을 유지할지 여부에 따라 달라집니다.

- **기존 데이터베이스와 함께 View Composer 마이그레이션**

View Composer를 다른 물리적 또는 가상 시스템으로 마이그레이션할 경우 현재 연결된 클론 가상 시스템을 유지하려면 새 VMware Horizon View Composer 서비스가 계속해서 기존 View Composer 데이터베이스를 사용해야 합니다.

- **연결된 클론 가상 시스템 없이 View Composer 마이그레이션**

연결된 클론 가상 시스템을 현재 VMware Horizon View Composer 서비스에서 관리하지 않는 경우 RSA 키를 새 시스템으로 마이그레이션하지 않고도 View Composer를 새 물리적 또는 가상 시스템으로 마이그레이션할 수 있습니다. 마이그레이션된 VMware Horizon View Composer 서비스를 원래 View Composer 데이터베이스에 연결하거나 View Composer를 위한 새 데이터베이스를 준비할 수 있습니다.

- **RSA 키 마이그레이션을 위해 Microsoft .NET Framework 준비**

기존 View Composer 데이터베이스를 사용하려면 시스템 간에 RSA 키 컨테이너를 마이그레이션해야 합니다. Microsoft .NET Framework와 함께 제공된 ASP.NET IIS 등록 도구를 사용하여 RSA 키 컨테이너를 마이그레이션합니다.

- **새 View Composer 서비스로 RSA 키 컨테이너 마이그레이션**

기존 View Composer 데이터베이스를 사용하려면 기존 VMware Horizon View Composer 서비스가 있는 소스 물리적 시스템 또는 가상 시스템에서 새 VMware Horizon View Composer 서비스를 설치할 시스템으로 RSA 키 컨테이너를 마이그레이션해야 합니다.

View Composer 마이그레이션 지침

VMware Horizon View Composer 서비스를 마이그레이션할 때 수행하는 단계는 기존의 연결된 클론 가상 시스템을 유지할지 여부에 따라 달라집니다.

현재 배포에서 연결된 클론 가상 시스템을 유지하려면 새로운 가상 또는 물리적 시스템에 설치하는 VMware Horizon View Composer 서비스에서 기존 View Composer 데이터베이스를 계속 사용해야 합니다. View Composer 데이터베이스에는 연결된 클론을 생성, 프로비저닝, 유지 관리 및 삭제하는 데 필요한 데이터가 포함되어 있습니다.

VMware Horizon View Composer 서비스를 마이그레이션할 경우 View Composer 데이터베이스를 새 시스템으로 마이그레이션할 수도 있습니다.

View Composer 데이터베이스의 마이그레이션 여부에 상관 없이 VMware Horizon View Composer 서비스를 설치하는 새 시스템과 동일한 도메인 또는 신뢰할 수 있는 도메인에서 사용할 수 있는 시스템에 데이터베이스를 구성해야 합니다.

View Composer는 View Composer 데이터베이스에 저장된 인증 정보를 암호화 및 암호 해독할 RSA 키 쌍을 생성합니다. 이 데이터 소스가 새 VMware Horizon View Composer 서비스와 호환되도록 하려면 원래 VMware Horizon View Composer 서비스에서 생성된 RSA 키 컨테이너를 마이그레이션해야 합니다. 새 서비스를 설치하는 시스템으로 RSA 키 컨테이너를 가져와야 합니다.

현재 VMware Horizon View Composer 서비스가 연결된 클론 가상 시스템을 관리하지 않는 경우 기존 View Composer 데이터베이스를 사용하지 않고 서비스를 마이그레이션할 수 있습니다. 기존 데이터베이스를 사용할지 여부에 상관없이 RSA 키를 마이그레이션할 필요가 없습니다.

참고 VMware Horizon View Composer 서비스의 각 인스턴스마다 고유한 View Composer 데이터베이스가 있어야 합니다. 여러 VMware Horizon View Composer 서비스가 View Composer 데이터베이스를 공유할 수 없습니다.

기존 데이터베이스와 함께 View Composer 마이그레이션

View Composer를 다른 물리적 또는 가상 시스템으로 마이그레이션할 경우 현재 연결된 클론 가상 시스템을 유지하려면 새 VMware Horizon View Composer 서비스가 계속해서 기존 View Composer 데이터베이스를 사용해야 합니다.

다음 중 어느 방향으로 View Composer를 마이그레이션할 경우 이 절차의 단계를 따르십시오.

- vCenter Server 시스템에서 독립 실행형 시스템으로 마이그레이션
- 독립 실행형 시스템에서 vCenter Server 시스템으로 마이그레이션
- 한 독립 실행형 시스템에서 다른 독립 실행형 시스템으로 마이그레이션
- 한 vCenter Server 시스템에서 다른 vCenter Server 시스템으로 마이그레이션

VMware Horizon View Composer 서비스를 마이그레이션할 경우 View Composer 데이터베이스를 새 위치로 마이그레이션할 수도 있습니다. 예를 들어 현재 데이터베이스가 함께 마이그레이션하려는 vCenter Server 시스템에 있을 경우 View Composer 데이터베이스를 마이그레이션해야 할 수 있습니다.

새 시스템에 VMware Horizon View Composer 서비스를 설치할 경우 View Composer 데이터베이스에 연결하도록 서비스를 구성해야 합니다.

사전 요구 사항

- View Composer 마이그레이션 요구 사항을 숙지하십시오. [View Composer 마이그레이션 지침](#)의 내용을 참조하십시오.
- RSA 키 컨테이너를 새 VMware Horizon View Composer 서비스로 마이그레이션하는 단계를 숙지하십시오. 자세한 내용은 [RSA 키 마이그레이션을 위해 Microsoft .NET Framework 준비 및 새 View Composer 서비스로 RSA 키 컨테이너 마이그레이션](#)의 내용을 참조하십시오.
- Horizon 7 설치 문서에서 VMware Horizon View Composer 서비스를 설치하는 방법을 숙지하십시오.

- Horizon 7 설치 문서에서 View Composer에 대한 TLS 인증서를 구성하는 방법을 숙지하십시오.
- Horizon Administrator에서 View Composer를 구성하는 방법을 숙지하십시오. 자세한 내용은 [View Composer 설정 구성](#) 및 [View Composer 도메인 구성](#)의 내용을 참조하십시오.
- 모범 사례로, View Composer 마이그레이션에 사용하는 소스 및 대상 시스템이 동일한지, 동일한 관리자 자격 증명을 공유하는지 확인하십시오. 독립 실행형 시스템에서 View Composer가 이미 설치된 vCenter Server 시스템으로 View Composer를 마이그레이션할 경우 두 시스템에 사용되는 자격 증명에 따르면 View Composer 구성이 실패할 수 있습니다.

절차

- 1 VMware Horizon View Composer 서비스와 연결된 vCenter Server 인스턴스에서 가상 시스템 프로비저닝을 사용하지 않도록 설정하십시오.
 - a Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
 - b **vCenter Server** 탭에서 vCenter Server 인스턴스를 선택하고 **프로비저닝 사용 안 함**을 클릭합니다.
- 2 (선택 사항) View Composer 데이터베이스를 새 위치로 마이그레이션합니다.
이 단계를 수행해야 할 경우 데이터베이스 관리자에게 마이그레이션 지침을 문의하십시오.
- 3 현재 시스템에서 VMware Horizon View Composer 서비스를 제거합니다.
- 4 (선택 사항) 새 시스템으로 RSA 키 컨테이너를 마이그레이션합니다.
- 5 새 시스템에 VMware Horizon View Composer 서비스를 설치합니다.
설치 도중 원래 VMware Horizon View Composer 서비스에서 사용된 데이터베이스의 DSN을 지정합니다. 해당 데이터베이스의 ODBC 데이터 소스에 제공된 도메인 관리자 사용자 이름과 암호도 지정합니다.
데이터베이스를 마이그레이션한 경우 DSN과 데이터 소스 정보가 데이터베이스의 새 위치를 가리켜야 합니다. 데이터베이스를 마이그레이션했는지 여부에 관계없이 새 VMware Horizon View Composer 서비스가 연결된 클론에 대한 원래 데이터베이스 정보에 액세스할 수 있어야 합니다.
- 6 새 시스템에서 View Composer를 위한 SSL 서버 인증서를 구성합니다.
원래 시스템에서 View Composer를 위해 설치된 인증서를 복사할 수도 있고 새 인증서를 설치할 수도 있습니다.
- 7 Horizon Administrator에서 새 View Composer 설정을 구성합니다.
 - a Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
 - b **vCenter Server** 탭에서 이 View Composer 서비스와 연결된 vCenter Server 인스턴스를 선택하고 **편집**을 클릭합니다.

- c View Composer Server 설정 창에서 **편집**을 클릭하고 새로운 View Composer 설정을 제공합니다.
 새 시스템에 vCenter Server와 함께 View Composer를 설치하려면 **vCenter Server와 함께 설치된 View Composer**를 선택하십시오.
 독립 실행형 시스템에 View Composer를 설치하려면 **독립 실행형 View Composer Server**를 선택하고 View Composer 시스템의 FQDN과 View Composer 사용자의 사용자 이름 및 암호를 입력하십시오.
- d 도메인 창에서 **서버 정보 확인**을 클릭하고 필요에 따라 View Composer 도메인을 추가하거나 편집합니다.
- e **확인**을 클릭합니다.

연결된 클론 가상 시스템 없이 View Composer 마이그레이션

연결된 클론 가상 시스템을 현재 VMware Horizon View Composer 서비스에서 관리하지 않는 경우 RSA 키를 새 시스템으로 마이그레이션하지 않고도 View Composer를 새 물리적 또는 가상 시스템으로 마이그레이션할 수 있습니다. 마이그레이션된 VMware Horizon View Composer 서비스를 원래 View Composer 데이터베이스에 연결하거나 View Composer를 위한 새 데이터베이스를 준비할 수 있습니다.

사전 요구 사항

- Horizon 7 설치 문서에서 VMware Horizon View Composer 서비스를 설치하는 방법을 숙지하십시오.
- Horizon 7 설치 문서에서 View Composer에 대한 TLS 인증서를 구성하는 방법을 숙지하십시오.
- Horizon Administrator에서 View Composer를 제거하는 단계를 숙지하십시오. [Horizon 7에서 View Composer 제거](#)의 내용을 참조하십시오.

View Composer를 제거하려면 View Composer가 연결된 클론 데스크톱을 더 이상 관리하지 않는지를 먼저 확인해야 합니다. 연결된 클론이 남아 있는 경우에는 이를 삭제해야 합니다.

- Horizon Administrator에서 View Composer를 구성하는 방법을 숙지하십시오. 자세한 내용은 [View Composer 설정 구성](#) 및 [View Composer 도메인 구성](#)의 내용을 참조하십시오.

절차

- 1 Horizon Administrator에서 Horizon Administrator의 View Composer를 제거합니다.
 - a **View 구성 > 서버**를 선택합니다.
 - b **vCenter Server** 탭에서 View Composer 서비스와 연결된 vCenter Server 인스턴스를 선택하고 **편집**을 클릭합니다.
 - c View Composer Server 설정 창에서 **편집**을 클릭합니다.
 - d **View Composer 사용 안 함**을 선택하고 **확인**을 클릭합니다.
- 2 현재 시스템에서 VMware Horizon View Composer 서비스를 제거합니다.

3 새 시스템에 VMware Horizon View Composer 서비스를 설치합니다.

설치 도중, 원래 또는 새 View Composer 데이터베이스의 DSN에 연결하도록 View Composer를 구성합니다.

4 새 시스템에서 View Composer를 위한 TLS 서버 인증서를 구성합니다.

원래 시스템에서 View Composer를 위해 설치된 인증서를 복사할 수도 있고 새 인증서를 설치할 수도 있습니다.

5 Horizon Administrator에서 새 View Composer 설정을 구성합니다.

a Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.

b **vCenter Server** 탭에서 이 View Composer 서비스와 연결된 vCenter Server 인스턴스를 선택하고 **편집**을 클릭합니다.

c View Composer Server 설정 창에서 **편집**을 클릭합니다.

d 새 View Composer 설정을 입력합니다.

새 시스템에 vCenter Server와 함께 View Composer를 설치하려면 **vCenter Server와 함께 설치된 View Composer**를 선택하십시오.

독립 실행형 시스템에 View Composer를 설치하려면 **독립 실행형 View Composer Server**를 선택하고 View Composer 시스템의 FQDN과 View Composer 사용자의 사용자 이름 및 암호를 입력하십시오.

e 도메인 창에서 **서버 정보 확인**을 클릭하고 필요에 따라 View Composer 도메인을 추가하거나 편집합니다.

f **확인**을 클릭합니다.

RSA 키 마이그레이션을 위해 Microsoft .NET Framework 준비

기존 View Composer 데이터베이스를 사용하려면 시스템 간에 RSA 키 컨테이너를 마이그레이션해야 합니다. Microsoft .NET Framework와 함께 제공된 ASP.NET IIS 등록 도구를 사용하여 RSA 키 컨테이너를 마이그레이션합니다.

사전 요구 사항

.NET Framework를 다운로드하고 ASP.NET IIS 등록 도구에 대한 내용을 읽어봅니다.

<http://www.microsoft.com/net>을 방문하십시오.

절차

1 기존 데이터베이스와 연결된 VMware Horizon View Composer 서비스가 설치된 물리적 또는 가상 시스템에 .NET Framework를 설치합니다.

2 새 VMware Horizon View Composer 서비스를 설치할 대상 시스템에 .NET Framework를 설치합니다.

다음에 수행할 작업

대상 시스템에 RSA 키 컨테이너를 마이그레이션합니다. 새 [View Composer 서비스로 RSA 키 컨테이너 마이그레이션](#)의 내용을 참조하십시오.

새 View Composer 서비스로 RSA 키 컨테이너 마이그레이션

기존 View Composer 데이터베이스를 사용하려면 기존 VMware Horizon View Composer 서비스가 있는 소스 물리적 시스템 또는 가상 시스템에서 새 VMware Horizon View Composer 서비스를 설치할 시스템으로 RSA 키 컨테이너를 마이그레이션해야 합니다.

새 VMware Horizon View Composer 서비스를 설치하기 전에 이 절차를 수행해야 합니다.

사전 요구 사항

소스 및 대상 시스템에 Microsoft .NET Framework와 ASP.NET IIS 등록 도구가 설치되었는지 확인합니다. [RSA 키 마이그레이션을 위해 Microsoft .NET Framework 준비](#)의 내용을 참조하십시오.

절차

- 1 기존 VMware Horizon View Composer 서비스가 있는 소스 시스템에서 명령 프롬프트를 열고 %windir%\Microsoft.NET\Framework\v2.0xxxxx 디렉토리로 이동합니다.
- 2 aspnet_regiis 명령을 입력해 로컬 파일에 RSA 키 쌍을 저장하십시오.
aspnet_regiis -px "SviKeyContainer" "keys.xml" -pri
ASP.NET IIS 등록 도구는 SviKeyContainer 컨테이너에서 RSA 공개-개인 키 쌍을 keys.xml 파일로 내보내고 로컬로 저장합니다.
- 3 새 VMware Horizon View Composer 서비스를 설치할 대상 시스템에 keys.xml 파일을 복사합니다.
- 4 대상 시스템에서 명령 프롬프트를 열고 %windir%\Microsoft.NET\Framework\v2.0xxxxx 디렉토리로 이동합니다.
- 5 RSA 키 쌍 데이터를 마이그레이션하려면 aspnet_regiis 명령을 입력하십시오.

aspnet_regiis -pi "SviKeyContainer" "path\keys.xml" -exp

여기서 path는 파일을 내보낼 경로입니다.

-exp 옵션은 내보낼 수 있는 키 쌍을 생성합니다. 나중에 마이그레이션이 필요할 경우 이 시스템에서 키를 내보내 다른 시스템으로 가져올 수 있습니다. 이전에 -exp 옵션을 사용하지 않고 키를 이 시스템으로 마이그레이션한 경우 키를 나중에 내보낼 수 있도록 -exp 옵션을 사용해 키를 다시 가져올 수 있습니다.

등록 도구는 키 쌍 데이터를 로컬 키 컨테이너로 가져옵니다.

다음에 수행할 작업

대상 시스템에 새 VMware Horizon View Composer 서비스를 설치합니다. View Composer가 원래 VMware Horizon View Composer 서비스에 사용된 것과 동일한 데이터베이스 정보에 연결할 수 있도록 DSN 및 ODBC 데이터 소스 정보를 입력합니다. 자세한 설치 지침은 Horizon 7 설치 문서의 “View Composer 설치”를 참조하십시오.

View Composer를 새 시스템으로 마이그레이션하고 동일한 데이터베이스를 사용하여 단계를 완료합니다. [기존 데이터베이스와 함께 View Composer 마이그레이션](#)의 내용을 참조하십시오.

연결 서버 인스턴스, 보안 서버 또는 View Composer의 인증서 업데이트

업데이트된 서버 TLS 인증서 또는 중간 인증서를 수신할 경우, 인증서를 각 연결 서버, 보안 서버 또는 View Composer 호스트의 Windows 로컬 컴퓨터 인증서 저장소로 가져오십시오.

일반적으로 서버 인증서는 12개월 후 만료됩니다. 루트 및 중간 인증서는 5년 또는 10년 후 만료됩니다.

서버 및 중간 인증서를 가져오는 방법에 대한 자세한 내용은 Horizon 7 설치 문서의 “새로운 TLS 인증서를 사용하도록 Horizon 연결 서버, 보안 서버 또는 View Composer 구성”을 참조하십시오.

사전 요구 사항

- 현재 유효한 인증서가 만료되기 전에 CA에서 업데이트된 서버 및 중간 인증서를 구하십시오.
- 인증서 스냅인이 연결 서버 인스턴스, 보안 서버 또는 VMware Horizon View Composer 서비스가 설치된 Windows Server의 MMC에 추가되었는지 확인합니다.

절차

- 1 서명된 TLS 서버 인증서를 Windows Server 호스트의 Windows 로컬 컴퓨터 인증서 저장소로 가져옵니다.
 - a 인증서 스냅인에서 서버 인증서를 **인증서(로컬 컴퓨터) > 개인 > 인증서** 폴더로 가져옵니다.
 - b 이 키를 **내보낼 수 있도록 표시**를 선택합니다.
 - c **다음, 마침**을 차례로 클릭합니다.
- 2 연결 서버 또는 보안 서버의 경우 Horizon 7 Server에 발급된 기존 인증서의 인증서 대화명인 **vdm**을 삭제하십시오.
 - a 기존 인증서를 마우스 오른쪽 단추로 클릭하고 **속성**을 클릭합니다.
 - b 일반 탭에서 대화명 텍스트인 **vdm**을 삭제합니다.
- 3 연결 서버 또는 보안 서버의 경우 이전 인증서를 대체하는 새 인증서에 인증서 대화명인 **vdm**을 추가하십시오.
 - a 새 인증서를 마우스 오른쪽 단추로 클릭하고 **속성**을 클릭합니다.
 - b 일반 탭의 대화명 필드에 **vdm**을 입력합니다.
 - c **적용**과 **확인**을 차례로 클릭합니다.

- 4 View Composer에 대해 발급된 서버 인증서의 경우 SviConfig ReplaceCertificate 유틸리티를 실행하여 View Composer가 사용하는 포트에 새 인증서를 바인딩합니다.

이 유틸리티는 새 인증서 바인딩에 바인딩된 기존 인증서를 대체합니다.

- a VMware Horizon View Composer 서비스를 중지합니다.
- b Windows 명령 프롬프트를 열고 SviConfig 실행 파일로 이동합니다.

파일은 View Composer 애플리케이션으로 찾을 수 있습니다. 기본 경로는 C:\Program Files (x86)\VMware\VMware View Composer\sviconfig.exe입니다.

- c SviConfig ReplaceCertificate 명령을 입력합니다. 예:

```
sviconfig -operation=ReplaceCertificate
          -delete=false
```

유틸리티가 Windows 로컬 컴퓨터 인증서 저장소에서 사용할 수 있는 TLS 인증서 번호 목록을 표시합니다.

- d 인증서를 선택하려면 인증서 번호를 입력하고 Enter를 누르십시오.

- 5 중간 인증서가 연결 서버, 보안 서버 또는 View Composer 호스트에 발급된 경우 가장 최근의 중간 인증서 업데이트를 Windows 인증서 저장소의 **인증서(로컬 컴퓨터) > 중간 인증 기관 > 인증서** 폴더로 가져오십시오.
- 6 변경 내용을 적용하기 위해 VMware Horizon View 연결 서버 서비스, VMware Horizon View 보안 서버 서비스 또는 VMware Horizon View Composer 서비스를 다시 시작합니다.

고객 환경 향상 프로그램

이 제품은 VMware의 CEIP(고객 환경 향상 프로그램)에 참여합니다. 이 제품에 대해 CEIP 가입 또는 탈퇴를 선택할 수 있습니다.

CEIP를 통해 수집된 데이터 및 이 데이터가 VMware에서 사용되는 용도와 관련된 세부 정보는 <http://www.vmware.com/trustvmware/ceip.html>의 신뢰 및 보증 센터에 명시되어 있습니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 제품 라이선싱 및 사용량**을 선택합니다.
- 2 **고객 환경 개선 프로그램** 패널에서 **설정 편집**을 클릭합니다.
- 3 CEIP에 가입하려면 **VMware 고객 환경 향상 프로그램 가입**을 선택합니다.
이 옵션을 선택하지 않으면 CEIP에 가입할 수 없습니다.
- 4 **확인**을 클릭합니다.

Horizon Administrator에서 ThinApp 애플리케이션 관리

9

Horizon Administrator를 사용하여 VMware ThinApp으로 패키지된 애플리케이션을 배포하고 관리할 수 있습니다. Horizon Administrator에서 ThinApp 애플리케이션을 관리하는 작업에는 애플리케이션 패키지 캡처 및 저장, Horizon Administrator에 ThinApp 애플리케이션 추가, 시스템 및 데스크톱 풀에 ThinApp 애플리케이션 할당 등의 작업이 포함됩니다.

Horizon Administrator에서 ThinApp 관리 기능을 사용하려면 라이선스가 있어야 합니다.

중요 ThinApp을 시스템 및 데스크톱 풀에 할당하여 배포하는 대신 ThinApp을 Active Directory 사용자와 그룹에 할당하려는 경우에는 VMware Identity Manager를 사용하면 됩니다.

본 장은 다음 항목을 포함합니다.

- [ThinApp 애플리케이션을 위한 Horizon 7 요구 사항](#)
- [애플리케이션 패키지 캡처 및 저장](#)
- [시스템 및 데스크톱 풀에 ThinApp 애플리케이션 할당](#)
- [Horizon Administrator에서 ThinApp 애플리케이션 유지 관리](#)
- [Horizon Administrator에서 ThinApp 애플리케이션 모니터링 및 문제 해결](#)
- [ThinApp 구성 예](#)

ThinApp 애플리케이션을 위한 Horizon 7 요구 사항

Horizon Administrator에서 원격 데스크톱에 배포될 ThinApp 애플리케이션을 캡처 및 저장할 경우 특정 요구 사항을 만족해야 합니다.

- MSI(Microsoft Installation) 패키지로 애플리케이션을 패키징해야 합니다.
- ThinApp 버전 4.6 이상을 사용하여 MSI 패키지를 생성하거나 다시 패키징해야 합니다.
- 연결 서버 호스트 및 원격 데스크톱에 액세스할 수 있는 Active Directory 도메인의 Windows 네트워크 공유에 MSI 패키지를 저장해야 합니다. 파일 서버는 컴퓨터 계정을 기반으로 한 파일 사용 권한 및 인증을 지원해야 합니다.
- MSI 패키지를 호스트하는 네트워크 공유에서 파일 및 공유 사용 권한을 구성하여 내장된 Active Directory 그룹 도메인 컴퓨터에 읽기 액세스를 제공해야 합니다. ThinApp 애플리케이션을 도메인 컨트롤러에 배포할 경우 내장 Active Directory 그룹 도메인 컨트롤러에 읽기 액세스를 제공해야 합니다.

- 사용자가 ThinApp 애플리케이션 패키지 스트리밍에 액세스할 수 있으려면 ThinApp 패키지를 호스팅하는 네트워크 공유의 NTFS 권한을 사용자를 위해 읽기 및 실행으로 설정합니다.
- 연결되지 않은 네임스페이스는 도메인 구성원 컴퓨터가 MSI 패키지를 호스팅하는 네트워크 공유에 액세스하지 못하도록 방지해야 합니다. 연결되지 않은 네임스페이스는 Active Directory 도메인 이름이 해당 도메인의 시스템에서 사용하는 DNS 네임스페이스와 다른 경우에 발생합니다. 자세한 내용은 VMware 기술 자료(KB) 문서 1023309에 나와 있습니다.
- 원격 데스크톱에서 스트리밍된 ThinApp 애플리케이션을 실행하려면 사용자에게 MSI 패키지를 호스팅하는 네트워크 공유에 대한 액세스 권한이 있어야 합니다.

애플리케이션 패키지 캡처 및 저장

ThinApp은 기본 운영 체제와 라이브러리, 프레임워크에서 애플리케이션을 분리하고 해당 애플리케이션을 단일 실행 파일로 묶어 애플리케이션 패키지를 생성함으로써 애플리케이션을 가상화합니다.

Horizon Administrator의 ThinApp 애플리케이션을 관리하려면 ThinApp **Setup Capture** 마법사를 사용해 애플리케이션을 MSI 형식으로 캡처 및 패키징하고 애플리케이션 저장소에 MSI 패키지를 저장해야 합니다.

애플리케이션 저장소는 Windows 네트워크 공유입니다. 네트워크 공유를 애플리케이션 저장소로 등록하려면 Horizon Administrator를 사용합니다. 여러 애플리케이션 저장소를 등록할 수 있습니다.

참고 애플리케이션 저장소가 여러 개인 경우 타사 솔루션을 사용해 로드 밸런싱과 가용성을 관리할 수 있습니다. Horizon 7에는 로드 밸런싱 또는 가용성 솔루션이 포함되어 있지 않습니다.

ThinApp 기능과 ThinApp **Setup Capture** 마법사 사용 방법에 대한 자세한 내용은 Introduction to VMware ThinApp(VMware ThinApp 소개) 및 ThinApp User's Guide(ThinApp 사용자 설명서)를 참조하십시오.

1 애플리케이션 패키징

ThinApp **Setup Capture** 마법사를 사용하여 애플리케이션을 캡처하고 패키징합니다.

2 Windows 네트워크 공유 생성

Horizon Administrator의 원격 데스크톱 및 풀에 배포된 MSI 패키지를 호스팅하려면 Windows 네트워크 공유를 생성해야 합니다.

3 애플리케이션 저장소 등록

Horizon Administrator의 애플리케이션 저장소로 MSI 패키지를 호스팅하는 Windows 네트워크 공유를 등록해야 합니다.

4 Horizon Administrator에 ThinApp 애플리케이션 추가

애플리케이션 저장소를 검사하고 ThinApp 애플리케이션을 선택해 Horizon Administrator에 ThinApp 애플리케이션을 추가합니다. Horizon Administrator에 ThinApp 애플리케이션을 추가한 후에는 해당 애플리케이션을 시스템 및 데스크톱 풀에 할당할 수 있습니다.

5 ThinApp 템플릿 생성

Horizon Administrator에 템플릿을 생성해 ThinApp 애플리케이션 그룹을 지정할 수 있습니다. 템플릿을 사용해 기능, 공급업체 또는 조직에 적합한 기타 논리적 그룹으로 애플리케이션을 묶을 수 있습니다.

애플리케이션 패키징

ThinApp **Setup Capture** 마법사를 사용하여 애플리케이션을 캡처하고 패키징합니다.

사전 요구 사항

- <http://www.vmware.com/products/thinapp>에서 ThinApp 소프트웨어를 다운로드하여 클린 컴퓨터에 설치하십시오. View에서 ThinApp 버전 4.6 이상이 지원됩니다.
- ThinApp User's Guide(ThinApp 사용자 설명서)의 ThinApp 소프트웨어 요구 사항 및 애플리케이션 패키징 지침을 숙지합니다.

절차

- 1 ThinApp **Setup Capture** 마법사를 시작하여 마법사의 프롬프트에 따르십시오.
- 2 ThinApp **Setup Capture** 마법사에서 프로젝트 위치에 대해 묻는 메시지가 나타날 경우 **MSI 패키지 빌드**를 선택합니다.
- 3 원격 데스크톱에 애플리케이션을 스트리밍하려는 경우 package.ini 파일에서 MSIStreaming 속성을 1로 설정합니다.

```
MSIStreaming=1
```

ThinApp **Setup Capture** 마법사는 애플리케이션, 애플리케이션을 실행하기 위해 필요한 모든 구성 요소 및 애플리케이션 자체를 MSI 패키지로 캡슐화합니다.

다음에 수행할 작업

Windows 네트워크 공유를 생성하여 MSI 패키지를 저장하십시오.

Windows 네트워크 공유 생성

Horizon Administrator의 원격 데스크톱 및 풀에 배포된 MSI 패키지를 호스팅하려면 Windows 네트워크 공유를 생성해야 합니다.

사전 요구 사항

- 애플리케이션을 패키지로 만들려면 ThinApp **설치 캡처** 마법사를 사용하십시오.
- 네트워크 공유가 ThinApp 애플리케이션 저장에 필요한 Horizon 7 요구 사항을 충족하는지 확인합니다. 자세한 내용은 [ThinApp 애플리케이션을 위한 Horizon 7 요구 사항](#)에 나와 있습니다.

절차

- 1 연결 서버 호스트와 원격 데스크톱 모두에 액세스할 수 있는 Active Directory 도메인의 컴퓨터에 공유 폴더를 생성합니다.

- 2 기본 Active Directory 그룹 도메인 컴퓨터에 대한 읽기 액세스를 허용하려면 공유 폴더에서 파일 및 공유 사용 권한을 구성하십시오.
- 3 도메인 컨트롤러에 ThinApp 애플리케이션을 할당하려면 기본 Active Directory 그룹 도메인 컨트롤러에 대한 읽기 액세스를 허용하십시오.
- 4 ThinApp 애플리케이션 패키지 스트리밍을 사용하려면 ThinApp 패키지를 호스팅하는 네트워크 공유의 NTFS 사용 권한을 사용자에게 대해 읽기 및 실행으로 설정하십시오.
- 5 MSI 패키지를 공유 폴더에 복사합니다.

다음에 수행할 작업

Windows 네트워크 공유를 애플리케이션 저장소로 Horizon Administrator에 등록하십시오.

애플리케이션 저장소 등록

Horizon Administrator의 애플리케이션 저장소로 MSI 패키지를 호스트하는 Windows 네트워크 공유를 등록해야 합니다.

여러 애플리케이션 저장소를 등록할 수 있습니다.

사전 요구 사항

Windows 네트워크 공유를 생성하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > ThinApp 구성**을 선택하고 **저장소 추가**를 클릭합니다.
- 2 **디스플레이 이름** 텍스트 상자에 애플리케이션 저장소의 디스플레이 이름을 입력하십시오.
- 3 **공유 경로** 텍스트 상자에 애플리케이션 패키지를 호스트하는 Windows 네트워크 공유에 대한 경로를 입력하십시오.

네트워크 공유 경로는 \\ServerComputerName\ShareName 형식이어야 하며 여기서 ServerComputerName은 서버 컴퓨터의 DNS 이름입니다. IP 주소를 지정하지 마십시오.

예: \\wwwserver.domain.com\\MSIPackages

- 4 **저장**을 클릭하여 Horizon Administrator로 애플리케이션 저장소를 등록합니다.

Horizon Administrator에 ThinApp 애플리케이션 추가

애플리케이션 저장소를 검사하고 ThinApp 애플리케이션을 선택해 Horizon Administrator에 ThinApp 애플리케이션을 추가합니다. Horizon Administrator에 ThinApp 애플리케이션을 추가한 후에는 해당 애플리케이션을 시스템 및 데스크톱 풀에 할당할 수 있습니다.

사전 요구 사항

Horizon Administrator에서 애플리케이션 저장소를 등록하십시오.

절차

1 Horizon Administrator에서 **카탈로그 > ThinApp**을 선택합니다.

2 **요약** 탭에서 **새 ThinApp 검사**를 클릭합니다.

3 검사를 할 애플리케이션 저장소와 폴더를 선택하고 **다음**을 클릭합니다.

애플리케이션 저장소에 하위 폴더가 있는 경우 루트 폴더를 확장하고 하위 폴더를 선택할 수 있습니다.

4 Horizon Administrator에 추가할 ThinApp 애플리케이션을 선택합니다.

ThinApp 애플리케이션을 여러 개 선택하려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다.

5 선택한 MSI 패키지 검사를 시작하려면 **검사**를 클릭합니다.

검사를 중지하려면 **검사 중지**를 클릭합니다.

Horizon Administrator에서 각 검사 작업 상태 및 Horizon Administrator에 추가된 ThinApp 애플리케이션 수를 보고합니다. Horizon Administrator에 이미 있는 애플리케이션을 선택하면 다시 추가되지 않습니다.

6 **마침**을 클릭합니다.

요약 탭에 새 ThinApp 애플리케이션이 표시됩니다.

다음에 수행할 작업

(선택 사항) ThinApp 템플릿을 생성하십시오.

ThinApp 템플릿 생성

Horizon Administrator에 템플릿을 생성해 ThinApp 애플리케이션 그룹을 지정할 수 있습니다. 템플릿을 사용해 기능, 공급업체 또는 조직에 적합한 기타 논리적 그룹으로 애플리케이션을 묶을 수 있습니다.

ThinApp 템플릿을 사용해 여러 애플리케이션을 간단하게 배포할 수 있습니다. 시스템 또는 데스크톱 풀에 ThinApp 템플릿을 할당하면 Horizon Administrator에서 현재 템플릿에 있는 모든 애플리케이션을 설치합니다.

ThinApp 템플릿 생성은 선택 사항입니다.

참고 시스템 또는 데스크톱 풀에 ThinApp 템플릿을 할당한 후에 템플릿에 애플리케이션을 추가하면 Horizon Administrator는 시스템 또는 데스크톱 풀에 새 애플리케이션을 자동으로 할당하지 않습니다. 시스템이나 데스크톱 풀에 이전에 할당한 ThinApp 템플릿에서 애플리케이션을 제거해도 해당 애플리케이션은 시스템 또는 데스크톱 풀에 할당된 채로 남아 있습니다.

사전 요구 사항

Horizon Administrator에 선택한 ThinApp 애플리케이션을 추가하십시오.

절차

1 Horizon Administrator에서 **카탈로그 > ThinApp**을 선택한 후 **새 템플릿**을 클릭합니다.

- 2 템플릿 이름을 입력하고 **추가**를 클릭합니다.

사용할 수 있는 모든 ThinApp 애플리케이션이 테이블에 표시됩니다.

- 3 특정 ThinApp 애플리케이션을 찾으려면 **찾기** 텍스트 상자에 애플리케이션 이름을 입력하고 **찾기**를 클릭합니다.
- 4 템플릿에 포함시킬 ThinApp 애플리케이션을 선택하고 **추가**를 클릭합니다.
애플리케이션을 여러 개 선택하려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다.
- 5 템플릿을 저장하려면 **확인**을 클릭합니다.

시스템 및 데스크톱 풀에 ThinApp 애플리케이션 할당

원격 데스크톱에 ThinApp 애플리케이션을 설치하려면 Horizon Administrator를 사용해 시스템 또는 데스크톱 풀에 ThinApp 애플리케이션을 할당해야 합니다.

시스템에 ThinApp 애플리케이션을 할당하면 몇 분 후에 Horizon Administrator에서 가상 시스템에 애플리케이션 설치를 시작합니다. 데스크톱 풀에 ThinApp 애플리케이션을 할당하는 경우에는 사용자가 풀의 원격 데스크톱에 처음 로그인할 때 Horizon Administrator에서 애플리케이션 설치를 시작합니다.

스트리밍

Horizon Administrator에서 원격 데스크톱에 ThinApp 애플리케이션의 바로 가기를 설치합니다. 바로 가기는 저장소를 호스팅하는 네트워크 공유에 있는 ThinApp 애플리케이션을 가리킵니다. 스트리밍된 ThinApp 애플리케이션을 실행하려면 사용자가 네트워크 공유에 액세스할 수 있어야 합니다.

전체

Horizon Administrator에서 로컬 파일 시스템에 전체 ThinApp 애플리케이션을 설치합니다.

애플리케이션 크기에 따라 ThinApp 애플리케이션 설치 시간이 다릅니다.

중요 vCenter Server 가상 시스템이 포함된 가상 시스템 기반 데스크톱과 자동화된 데스크톱 풀 또는 수동 풀에 ThinApp 애플리케이션을 할당할 수 있습니다. 게시된 데스크톱이나 기존 PC에는 ThinApp 애플리케이션을 할당할 수 없습니다.

■ ThinApp 애플리케이션 할당에 대한 모범 사례

시스템 및 데스크톱 풀에 ThinApp 애플리케이션을 할당할 때는 다음과 같은 모범 사례를 따르는 것이 좋습니다.

■ 다중 시스템에 ThinApp 애플리케이션 할당

특정 ThinApp을 하나 이상의 시스템에 할당할 수 있습니다.

■ 시스템에 다중 ThinApp 애플리케이션 할당

특정 시스템에 하나 이상의 ThinApp 애플리케이션을 할당할 수 있습니다.

■ 다중 데스크톱 풀에 ThinApp 애플리케이션 할당

특정 ThinApp 애플리케이션을 하나 이상의 데스크톱 풀에 할당할 수 있습니다.

- **데스크톱 풀에 다중 ThinApp 애플리케이션 할당**

특정 데스크톱 풀에 하나 이상의 ThinApp 애플리케이션을 할당할 수 있습니다.

- **시스템 또는 데스크톱 풀에 ThinApp 템플릿 할당**

시스템 또는 데스크톱 풀에 ThinApp 템플릿을 할당해 다중 ThinApp 애플리케이션 배포 작업을 간소화할 수 있습니다.

- **ThinApp 애플리케이션 할당 검토**

현재 특정 ThinApp 애플리케이션이 할당되어 있는 모든 시스템 및 데스크톱 풀을 검토할 수 있습니다. 또한 특정 시스템 또는 데스크톱 풀에 할당되어 있는 모든 ThinApp 애플리케이션을 검토할 수도 있습니다.

- **MSI 패키지 정보 표시**

Horizon Administrator에 ThinApp 애플리케이션을 추가한 후에 MSI 패키지 정보를 표시할 수 있습니다.

ThinApp 애플리케이션 할당에 대한 모범 사례

시스템 및 데스크톱 풀에 ThinApp 애플리케이션을 할당할 때는 다음과 같은 모범 사례를 따르는 것이 좋습니다.

- 특정 원격 데스크톱에 ThinApp 애플리케이션을 설치하려면 데스크톱을 호스트하는 가상 시스템에 애플리케이션을 할당하십시오. 시스템에 일반 이름 지정 규칙을 사용할 경우 시스템 할당을 사용하여, 해당 이름 지정 규칙을 사용하는 모든 시스템에 애플리케이션을 신속하게 배포할 수 있습니다.
- 데스크톱 풀의 모든 시스템에 ThinApp 애플리케이션을 설치하려면 데스크톱 풀에 애플리케이션을 할당하십시오. 부서 또는 사용자 유형별로 데스크톱 풀을 구성하면 데스크톱 풀 할당을 사용하여 특정 부서나 사용자에게 애플리케이션을 신속하게 배포할 수 있습니다. 예를 들어, 회계 부서 사용자용 데스크톱 풀이 있는 경우, 회계 부서 풀에 애플리케이션을 할당하여 회계 부서의 모든 사용자에게 동일한 애플리케이션을 배포할 수 있습니다.
- 여러 ThinApp 애플리케이션을 간소하게 배포하려면 해당 애플리케이션을 ThinApp 템플릿에 포함시키십시오. ThinApp 템플릿을 시스템 또는 데스크톱 풀에 할당하면 Horizon Administrator는 현재 템플릿에 있는 모든 애플리케이션을 설치합니다.
- 시스템 또는 데스크톱 풀에 이미 할당된 ThinApp 애플리케이션이 템플릿에 포함되어 있는 경우에는 해당 시스템 또는 데스크톱 풀에 ThinApp 템플릿을 할당하지 마십시오. 또한 동일한 시스템이나 데스크톱 풀에 다른 설치 유형으로 ThinApp 템플릿을 두 번 이상 할당하지 마십시오. Horizon Administrator는 이 두 경우에 ThinApp 할당 오류를 반환합니다.

다중 시스템에 ThinApp 애플리케이션 할당

특정 ThinApp을 하나 이상의 시스템에 할당할 수 있습니다.

사전 요구 사항

애플리케이션 저장소를 검사하고 선택한 ThinApp 애플리케이션을 Horizon Administrator에 추가하십시오. [Horizon Administrator에 ThinApp 애플리케이션 추가](#)의 내용을 참조하십시오.

절차

- 1 Horizon Administrator에서 **카탈로그 > ThinApp**을 선택하고 ThinApp 애플리케이션을 선택합니다.

- 2 **할당 추가** 드롭다운 메뉴에서 **시스템 할당**을 선택합니다.

ThinApp 애플리케이션이 할당되지 않은 시스템이 테이블에 표시됩니다.

옵션	조치
특정 시스템 찾기	찾기 텍스트 상자에 시스템 이름을 입력하고 찾기 를 클릭합니다.
이름 지정 규칙이 동일한 시스템 모두 찾기	찾기 텍스트 상자에 시스템 이름 일부를 입력하고 찾기 를 클릭합니다.

- 3 ThinApp 애플리케이션을 할당할 시스템을 선택하고 **추가**를 클릭합니다.
시스템을 여러 개 선택하려면 Ctrl 또는 Shift 키를 누른 채 클릭하십시오.
- 4 설치 유형을 선택하고 **확인**을 클릭합니다.

옵션	조치
스트리밍	시스템에 애플리케이션의 바로 가기를 설치합니다. 바로 가기는 저장소를 호스팅하는 네트워크 공유에 있는 애플리케이션을 가리킵니다. 애플리케이션을 실행하려면 사용자가 네트워크 공유에 액세스할 수 있어야 합니다.
전체	시스템의 로컬 파일 시스템에 전체 애플리케이션을 설치합니다.

두 설치 유형을 모두 지원하지 않는 ThinApp 애플리케이션도 있습니다. 애플리케이션 패키지를 생성한 방법에 따라 사용할 수 있는 설치 유형이 다릅니다.

몇 분 후에 Horizon Administrator에서 ThinApp 애플리케이션 설치를 시작합니다. 설치가 완료되면 가상 시스템에서 호스팅되는 데스크톱의 모든 사용자가 애플리케이션을 사용할 수 있습니다.

시스템에 다중 ThinApp 애플리케이션 할당

특정 시스템에 하나 이상의 ThinApp 애플리케이션을 할당할 수 있습니다.

사전 요구 사항

애플리케이션 저장소를 검사하고 선택한 ThinApp 애플리케이션을 Horizon Administrator에 추가하십시오. [Horizon Administrator에 ThinApp 애플리케이션 추가](#)의 내용을 참조하십시오.

절차

- 1 Horizon Administrator에서 **리소스 > 시스템**을 선택하고 시스템 열에서 시스템 이름을 두 번 클릭합니다.
- 2 **요약** 탭의 ThinApp 창에서 **할당 추가**를 클릭합니다.
시스템에 할당되지 않은 ThinApp 애플리케이션이 테이블에 표시됩니다.
- 3 특정 애플리케이션을 찾으려면 **찾기** 텍스트 상자에 애플리케이션 이름을 입력하고 **찾기**를 클릭합니다.

- 4 시스템에 할당할 ThinApp 애플리케이션을 선택하고 **추가**를 클릭합니다.

애플리케이션을 여러 개 추가하려면 이 단계를 반복하십시오.

- 5 설치 유형을 선택하고 **확인**을 클릭합니다.

옵션	조치
스트리밍	시스템에 애플리케이션의 바로 가기를 설치합니다. 바로 가기는 저장소를 호스팅하는 네트워크 공유에 있는 애플리케이션을 가리킵니다. 애플리케이션을 실행하려면 사용자가 네트워크 공유에 액세스할 수 있어야 합니다.
전체	시스템의 로컬 파일 시스템에 전체 애플리케이션을 설치합니다.

두 설치 유형을 모두 지원하지 않는 ThinApp 애플리케이션도 있습니다. 애플리케이션 패키지를 생성한 방법에 따라 사용할 수 있는 설치 유형이 다릅니다.

몇 분 후에 Horizon Administrator에서 ThinApp 애플리케이션 설치를 시작합니다. 설치를 완료하면 가상 시스템에서 호스팅되는 데스크톱의 모든 사용자가 해당 애플리케이션을 사용할 수 있습니다.

다중 데스크톱 풀에 ThinApp 애플리케이션 할당

특정 ThinApp 애플리케이션을 하나 이상의 데스크톱 풀에 할당할 수 있습니다.

연결된 클론 풀에 ThinApp 애플리케이션을 할당하고 나중에 풀을 새로 고침, 재구성 또는 재조정하는 경우에는 Horizon Administrator가 대신해서 애플리케이션을 다시 설치합니다. 수동으로 애플리케이션을 다시 설치할 필요가 없습니다.

사전 요구 사항

애플리케이션 저장소를 검사하고 선택한 ThinApp 애플리케이션을 Horizon Administrator에 추가하십시오. [Horizon Administrator에 ThinApp 애플리케이션 추가](#)의 내용을 참조하십시오.

절차

- Horizon Administrator에서 **카탈로그 > ThinApp**을 선택하고 ThinApp 애플리케이션을 선택합니다.
- 할당 추가** 드롭다운 메뉴에서 **데스크톱 풀 할당**을 선택합니다.

ThinApp 애플리케이션이 아직 할당되지 않은 데스크톱 풀이 테이블에 표시됩니다.

옵션	조치
특정 데스크톱 풀 찾기	찾기 텍스트 상자에 데스크톱 풀 이름을 입력하고 찾기 를 클릭합니다.
이름 지정 규칙이 동일한 데스크톱 풀 모두 찾기	찾기 텍스트 상자에 데스크톱 풀 이름의 일부를 입력하고 찾기 를 클릭합니다.

- ThinApp 애플리케이션을 할당할 데스크톱 풀을 선택하고 **추가**를 클릭합니다.

데스크톱 풀을 여러 개 선택하려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다.

4 설치 유형을 선택하고 **확인**을 클릭합니다.

옵션	조치
스트리밍	시스템에 애플리케이션의 바로 가기를 설치합니다. 바로 가기는 저장소를 호스팅하는 네트워크 공유에 있는 애플리케이션을 가리킵니다. 애플리케이션을 실행하려면 사용자가 네트워크 공유에 액세스할 수 있어야 합니다.
전체	시스템의 로컬 파일 시스템에 전체 애플리케이션을 설치합니다.

두 설치 유형을 모두 지원하지 않는 ThinApp 애플리케이션도 있습니다. 애플리케이션 패키지를 생성한 방법에 따라 사용할 수 있는 설치 유형이 다릅니다.

사용자가 풀의 데스크톱에 처음 로그인할 때 Horizon Administrator에서 ThinApp 애플리케이션 설치를 시작합니다. 설치가 완료되면 데스크톱 풀의 모든 사용자가 해당 애플리케이션을 사용할 수 있습니다.

데스크톱 풀에 다중 ThinApp 애플리케이션 할당

특정 데스크톱 풀에 하나 이상의 ThinApp 애플리케이션을 할당할 수 있습니다.

연결된 클론 풀에 ThinApp 애플리케이션을 할당하고 나중에 풀을 새로 고침, 재구성 또는 재조정하는 경우에는 Horizon Administrator가 대신해서 애플리케이션을 다시 설치합니다. 수동으로 애플리케이션을 다시 설치할 필요가 없습니다.

사전 요구 사항

애플리케이션 저장소를 검사하고 선택한 ThinApp 애플리케이션을 Horizon Administrator에 추가하십시오. [Horizon Administrator에 ThinApp 애플리케이션 추가](#)의 내용을 참조하십시오.

절차

- 1 Horizon Administrator에서 **카탈로그 > 데스크톱 풀**을 선택하고 풀 ID를 두 번 클릭합니다.
- 2 **인벤토리** 탭에서 **ThinApp**을 클릭한 다음 **할당 추가**를 클릭합니다.
풀에 할당되지 않은 ThinApp 애플리케이션이 테이블에 표시됩니다.
- 3 특정 애플리케이션을 찾으려면 **찾기** 텍스트 상자에 ThinApp 애플리케이션 이름을 입력하고 **찾기**를 클릭합니다.
- 4 풀에 할당할 ThinApp 애플리케이션을 선택하고 **추가**를 클릭합니다.
애플리케이션을 여러 개 선택하려면 이 단계를 반복하십시오.
- 5 설치 유형을 선택하고 **확인**을 클릭합니다.

옵션	조치
스트리밍	시스템에 애플리케이션의 바로 가기를 설치합니다. 바로 가기는 저장소를 호스팅하는 네트워크 공유에 있는 애플리케이션을 가리킵니다. 애플리케이션을 실행하려면 사용자가 네트워크 공유에 액세스할 수 있어야 합니다.
전체	시스템의 로컬 파일 시스템에 전체 애플리케이션을 설치합니다.

두 설치 유형을 모두 지원하지 않는 ThinApp 애플리케이션도 있습니다. 애플리케이션 패키지를 생성한 방법에 따라 사용할 수 있는 설치 유형이 다릅니다.

사용자가 풀의 데스크톱에 처음 로그인할 때 Horizon Administrator에서 ThinApp 애플리케이션 설치를 시작합니다. 설치가 완료되면 데스크톱 풀의 모든 사용자가 해당 애플리케이션을 사용할 수 있습니다.

시스템 또는 데스크톱 풀에 ThinApp 템플릿 할당

시스템 또는 데스크톱 풀에 ThinApp 템플릿을 할당해 다중 ThinApp 애플리케이션 배포 작업을 간소화할 수 있습니다.

시스템 또는 데스크톱 풀에 ThinApp 템플릿을 할당하는 경우에는 Horizon Administrator가 현재 템플릿에 있는 ThinApp 애플리케이션을 설치합니다.

사전 요구 사항

ThinApp 템플릿을 생성하십시오. [ThinApp 템플릿 생성](#)의 내용을 참조하십시오.

절차

- 1 Horizon Administrator에서 **카탈로그 > ThinApp**을 선택합니다.
- 2 ThinApp 템플릿을 선택합니다.
- 3 **할당 추가** 드롭다운 메뉴에서 **시스템 할당** 또는 **데스크톱 풀 할당**을 선택합니다.

모든 시스템 또는 데스크톱 풀이 테이블에 표시됩니다.

옵션	조치
특정 시스템 또는 데스크톱 풀 찾기	찾기 텍스트 상자에 시스템 또는 데스크톱 풀 이름을 입력하고 찾기 를 클릭합니다.
이름 지정 규칙이 동일한 시스템 또는 데스크톱 풀 모두 찾기	찾기 텍스트 상자에 시스템 또는 데스크톱 풀 이름의 일부를 입력하고 찾기 를 클릭합니다.

- 4 ThinApp 템플릿을 할당할 시스템 또는 데스크톱 풀을 선택하고 **추가**를 클릭합니다.

시스템 또는 데스크톱 풀을 여러 개 선택하려면 이 단계를 반복하십시오.

- 5 설치 유형을 선택하고 **확인**을 클릭합니다.

옵션	조치
스트리밍	시스템에 애플리케이션의 바로 가기를 설치합니다. 바로 가기는 저장소를 호스팅하는 네트워크 공유에 있는 애플리케이션을 가리킵니다. 애플리케이션을 실행하려면 사용자가 네트워크 공유에 액세스할 수 있어야 합니다.
전체	시스템의 로컬 파일 시스템에 전체 애플리케이션을 설치합니다.

두 설치 유형을 모두 지원하지 않는 ThinApp 애플리케이션도 있습니다. 애플리케이션 패키지를 생성한 방법에 따라 사용할 수 있는 설치 유형이 다릅니다.

시스템에 ThinApp 템플릿을 할당하면 몇 분 후에 Horizon Administrator에서 템플릿에 있는 애플리케이션 설치를 시작합니다. 데스크톱 풀에 ThinApp 템플릿을 할당하는 경우에는 사용자가 데스크톱 풀의 원격 데스크톱에 처음 로그인할 때 Horizon Administrator에서 템플릿에 있는 애플리케이션 설치를 시작합니다. 설치가 완료되면 시스템 또는 데스크톱 풀의 모든 사용자가 해당 애플리케이션을 사용할 수 있습니다.

시스템 또는 데스크톱 풀에 이미 할당된 애플리케이션이 ThinApp 템플릿에 포함되어 있는 경우에는 Horizon Administrator에서 애플리케이션 할당 오류를 반환합니다.

ThinApp 애플리케이션 할당 검토

현재 특정 ThinApp 애플리케이션이 할당되어 있는 모든 시스템 및 데스크톱 풀을 검토할 수 있습니다. 또한 특정 시스템 또는 데스크톱 풀에 할당되어 있는 모든 ThinApp 애플리케이션을 검토할 수도 있습니다.

사전 요구 사항

ThinApp 애플리케이션 설치 상태 값의 ThinApp 설치 상태 값을 숙지하십시오.

절차

- 검토할 ThinApp 애플리케이션 할당을 검토하십시오.

옵션	조치
특정 ThinApp 애플리케이션이 할당된 모든 시스템 및 데스크톱 풀 검토	<p>Catalog > ThinApps and double-click the name of the ThinApp application.</p> <p>할당 탭에 설치 유형을 포함하여 애플리케이션이 현재 할당된 시스템 및 데스크톱 풀이 표시됩니다.</p> <p>시스템 탭에는 설치 상태 정보를 포함하여 현재 애플리케이션과 연결된 시스템이 표시됩니다.</p> <p>참고 ThinApp 애플리케이션을 풀에 할당할 경우 애플리케이션이 설치된 후에만 풀의 시스템이 시스템 탭에 나타납니다.</p>
특정 시스템에 할당된 모든 ThinApp 애플리케이션 검토	<p>Resources > Machines and double-click the name of the machine in Machine column.</p> <p>요약 탭의 ThinApp 창에 설치 상태를 포함하여 현재 시스템에 할당된 각 애플리케이션이 표시됩니다.</p>
특정 데스크톱 풀에 할당된 모든 ThinApp 애플리케이션 검토	<p>카탈로그 > 데스크톱 풀을 선택한 다음, 풀 ID를 두 번 클릭하며, 인벤토리 탭을 선택하고, ThinApp을 클릭합니다.</p> <p>ThinApp 할당 창에 현재 데스크톱 풀에 할당된 각 애플리케이션이 표시됩니다.</p>

ThinApp 애플리케이션 설치 상태 값

시스템이나 풀에 ThinApp 애플리케이션을 할당하면 Horizon Administrator에 설치 상태가 표시됩니다.

다음 표에서는 각 상태 값을 설명합니다.

표 9-1. ThinApp 애플리케이션 설치 상태

상태	설명
할당됨	ThinApp 애플리케이션이 시스템에 할당되었습니다.
설치 오류	Horizon Administrator가 ThinApp 애플리케이션을 설치할 때 오류가 발생했습니다.
제거 오류	Horizon Administrator가 ThinApp 애플리케이션을 제거할 때 오류가 발생했습니다.
설치됨	ThinApp 애플리케이션이 설치되었습니다.
설치 보류 중	Horizon Administrator가 ThinApp 애플리케이션을 설치하려고 합니다. 이 상태에 있는 애플리케이션을 할당 해제할 수 없습니다. 참고 이 값은 데스크톱 풀에 포함된 시스템에 대해서는 표시되지 않습니다.
제거 보류 중	Horizon Administrator가 ThinApp 애플리케이션을 제거하려고 합니다.

MSI 패키지 정보 표시

Horizon Administrator에 ThinApp 애플리케이션을 추가한 후에 MSI 패키지 정보를 표시할 수 있습니다.

절차

- 1 Horizon Administrator에서 **카탈로그 > ThinApp**을 선택합니다.
현재 사용할 수 있는 애플리케이션 목록과 전체 및 스트리밍 할당 수가 **요약** 탭에 표시됩니다.
- 2 ThinApp 열에서 애플리케이션 이름을 두 번 클릭합니다.
- 3 MSI 패키지에 대한 일반 정보를 확인하려면 **요약** 탭을 선택합니다.
- 4 MSI 패키지에 대한 자세한 정보를 확인하려면 **패키지 정보**를 클릭합니다.

Horizon Administrator에서 ThinApp 애플리케이션 유지 관리

Horizon Administrator에서 ThinApp 애플리케이션을 유지 관리하는 작업에는 ThinApp 애플리케이션 할당 제거, ThinApp 애플리케이션 및 ThinApp 애플리케이션 저장소 제거, ThinApp 템플릿 수정 및 삭제 등이 포함됩니다.

참고 ThinApp 애플리케이션을 업그레이드하려면 이전 버전의 애플리케이션을 할당 해제 및 제거하고 새 버전을 추가 및 할당해야 합니다.

- **여러 시스템에서 ThinApp 애플리케이션 할당 제거**
하나 이상의 시스템에서 특정 ThinApp 애플리케이션에 대한 할당을 제거할 수 있습니다.
- **시스템에서 여러 ThinApp 애플리케이션 할당 제거**
특정 시스템에서 하나 이상의 ThinApp 애플리케이션에 대한 할당을 제거할 수 있습니다.
- **여러 데스크톱 풀에서 ThinApp 애플리케이션 할당 제거**
하나 이상의 데스크톱 풀에서 특정 ThinApp 애플리케이션에 대한 할당을 제거할 수 있습니다.

- **데스크톱 풀에서 여러 ThinApp 애플리케이션 할당 제거**

특정 데스크톱 풀에서 하나 이상의 ThinApp 애플리케이션 할당을 제거할 수 있습니다.

- **Horizon Administrator에서 ThinApp 애플리케이션 제거**

Horizon Administrator에서 ThinApp 애플리케이션을 제거할 경우 애플리케이션을 더 이상 시스템 및 데스크톱 풀에 할당할 수 없습니다.

- **ThinApp 템플릿 수정 또는 삭제**

ThinApp 템플릿에 애플리케이션을 추가 및 제거할 수 있습니다. ThinApp 템플릿을 삭제할 수도 있습니다.

- **애플리케이션 저장소 제거**

Horizon Administrator에서 애플리케이션 저장소를 제거할 수 있습니다.

여러 시스템에서 ThinApp 애플리케이션 할당 제거

하나 이상의 시스템에서 특정 ThinApp 애플리케이션에 대한 할당을 제거할 수 있습니다.

사전 요구 사항

애플리케이션을 제거할 시스템에서 호스팅되는 원격 데스크톱의 사용자에게 알립니다.

절차

- 1 Horizon Administrator에서 **카탈로그 > ThinApp**을 선택하고 ThinApp 애플리케이션의 이름을 두 번 클릭합니다.
- 2 **할당** 탭에서 시스템을 선택하고 **할당 제거**를 클릭합니다.

시스템을 여러 개 선택하려면 Ctrl 또는 Shift 키를 누른 채 클릭하십시오.

몇 분 후 Horizon Administrator로 ThinApp 애플리케이션이 제거됩니다.

중요 Horizon Administrator가 애플리케이션을 제거할 때 최종 사용자가 ThinApp 애플리케이션을 사용 중일 경우 제거가 실패하고 애플리케이션 상태는 제거 오류로 변경됩니다. 이 오류가 발생할 경우 먼저 시스템에서 ThinApp 애플리케이션 파일을 수동으로 제거한 후 Horizon Administrator에서 **데스크톱의 애플리케이션 상태 제거**를 클릭해야 합니다.

시스템에서 여러 ThinApp 애플리케이션 할당 제거

특정 시스템에서 하나 이상의 ThinApp 애플리케이션에 대한 할당을 제거할 수 있습니다.

사전 요구 사항

애플리케이션을 제거할 시스템에서 호스팅되는 원격 데스크톱에 대해 사용자에게 알립니다.

절차

- 1 Horizon Administrator에서 **리소스 > 시스템**을 선택하고 시스템 열에서 시스템 이름을 두 번 클릭합니다.

2 요약 탭에서 ThinApp 애플리케이션을 선택하고 ThinApps 창의 **할당 제거**를 클릭합니다.

이 단계를 반복하여 다른 애플리케이션 할당을 제거합니다.

몇 분 후 Horizon Administrator로 ThinApp 애플리케이션이 제거됩니다.

중요 Horizon Administrator가 애플리케이션을 제거할 때 최종 사용자가 ThinApp 애플리케이션을 사용 중일 경우 제거가 실패하고 애플리케이션 상태는 제거 오류로 변경됩니다. 이 오류가 발생할 경우 먼저 시스템에서 ThinApp 애플리케이션 파일을 수동으로 제거한 후 Horizon Administrator에서 **데스크톱의 애플리케이션 상태 제거**를 클릭해야 합니다.

여러 데스크톱 풀에서 ThinApp 애플리케이션 할당 제거

하나 이상의 데스크톱 풀에서 특정 ThinApp 애플리케이션에 대한 할당을 제거할 수 있습니다.

사전 요구 사항

애플리케이션을 제거할 풀의 원격 데스크톱 사용자에게 알립니다.

절차

1 Horizon Administrator에서 **카탈로그 > ThinApp**을 선택하고 ThinApp 애플리케이션의 이름을 두 번 클릭합니다.

2 할당 탭에서 데스크톱 풀을 선택하고 **할당 제거**를 클릭합니다.

데스크톱 풀을 여러 개 선택하려면 Ctrl 또는 Shift 키를 누른 채 클릭합니다.

Horizon Administrator는 풀의 원격 데스크톱에 사용자가 처음 로그인할 때 ThinApp 애플리케이션을 제거합니다.

데스크톱 풀에서 여러 ThinApp 애플리케이션 할당 제거

특정 데스크톱 풀에서 하나 이상의 ThinApp 애플리케이션 할당을 제거할 수 있습니다.

사전 요구 사항

애플리케이션을 제거할 풀의 원격 데스크톱 사용자에게 알립니다.

절차

1 Horizon Administrator에서 **카탈로그 > 데스크톱 풀**을 선택하고 풀 ID를 두 번 클릭합니다.

2 인벤토리 탭에서 **ThinApp**을 클릭하고 ThinApp 애플리케이션을 선택한 다음 **할당 제거**를 클릭합니다.

이 단계를 반복하여 여러 애플리케이션을 제거합니다.

Horizon Administrator는 풀의 원격 데스크톱에 사용자가 처음 로그인할 때 ThinApp 애플리케이션을 제거합니다.

Horizon Administrator에서 ThinApp 애플리케이션 제거

Horizon Administrator에서 ThinApp 애플리케이션을 제거할 경우 애플리케이션을 더 이상 시스템 및 데스크톱 풀에 할당할 수 없습니다.

조직에서 다른 공급업체의 애플리케이션으로 교체하기로 한 경우 ThinApp 애플리케이션을 제거해야 합니다.

참고 이미 시스템 또는 데스크톱 풀에 할당되었거나 제거 보류 중 상태인 경우 ThinApp 애플리케이션을 제거할 수 없습니다.

사전 요구 사항

ThinApp 애플리케이션이 현재 시스템 또는 데스크톱 풀에 할당된 경우 시스템 또는 데스크톱 풀에서 할당을 제거합니다.

절차

- 1 Horizon Administrator에서 **카탈로그 > ThinApp**을 선택하고 ThinApp 애플리케이션을 선택합니다.
- 2 **ThinApp 제거**를 클릭합니다.
- 3 **확인**을 클릭합니다.

ThinApp 템플릿 수정 또는 삭제

ThinApp 템플릿에 애플리케이션을 추가 및 제거할 수 있습니다. ThinApp 템플릿을 삭제할 수도 있습니다.

시스템 또는 데스크톱 풀에 ThinApp 템플릿을 할당한 후에 템플릿에 애플리케이션을 추가하면 Horizon Administrator는 시스템 또는 데스크톱 풀에 새 애플리케이션을 자동으로 할당하지 않습니다. 시스템이나 데스크톱 풀에 이전에 할당한 ThinApp 템플릿에서 애플리케이션을 제거해도 해당 애플리케이션은 시스템 또는 데스크톱 풀에 할당된 채로 남아 있습니다.

절차

- ◆ Horizon Administrator에서 **카탈로그 > ThinApp**을 선택하고 ThinApp 템플릿을 선택합니다.

옵션	조치
템플릿에서 ThinApp 애플리케이션 추가 또는 제거	템플릿 편집 을 클릭합니다.
템플릿 삭제	템플릿 제거 를 클릭합니다.

애플리케이션 저장소 제거

Horizon Administrator에서 애플리케이션 저장소를 제거할 수 있습니다.

포함된 MSI 패키지가 더 이상 필요하지 않거나 다른 네트워크 공유로 MSI 패키지를 이동시켜야 할 경우 애플리케이션 저장소를 제거해야 할 수 있습니다. Horizon Administrator에서는 애플리케이션 저장소의 공유 경로를 편집할 수 없습니다.

절차

- 1 Horizon Administrator에서 **View 구성 > ThinApp 구성**을 선택하고 애플리케이션 저장소를 선택합니다.
- 2 **저장소 제거**를 클릭합니다.

Horizon Administrator에서 ThinApp 애플리케이션 모니터링 및 문제 해결

Horizon Administrator는 ThinApp 애플리케이션 관리와 관련된 이벤트를 이벤트 및 보고 데이터베이스에 기록합니다. Horizon Administrator의 **이벤트** 페이지에서 이러한 이벤트를 볼 수 있습니다.

이벤트는 다음과 같은 경우에 **이벤트** 페이지에 표시됩니다.

- ThinApp 애플리케이션을 할당하거나 애플리케이션 할당을 제거합니다.
- 시스템에 ThinApp 애플리케이션을 설치하거나 제거합니다.
- ThinApp 애플리케이션을 설치 또는 제거할 수 없습니다.
- ThinApp 애플리케이션 저장소가 Horizon Administrator에서 등록, 수정 또는 제거됨
- ThinApp 애플리케이션이 Horizon Administrator에 추가됨

공통 ThinApp 애플리케이션 관리 문제 해결에 대한 문제 해결 팁을 사용할 수 있습니다.

애플리케이션 저장소를 등록할 수 없음

Horizon Administrator의 애플리케이션 저장소를 등록할 수 없습니다.

문제

Horizon Administrator의 애플리케이션 저장소를 등록하려고 할 때 오류 메시지를 받습니다.

원인

연결 서버 호스트가 애플리케이션 저장소를 호스팅하는 네트워크 공유에 액세스할 수 없습니다. **공유 경로** 텍스트 상자에 입력한 네트워크 공유 경로가 올바르지 않거나 애플리케이션 저장소를 호스팅하는 네트워크 공유가 연결 서버 호스트에서 액세스할 수 없는 도메인에 위치하거나 네트워크 공유 사용 권한을 제대로 설정하지 않았습니

해결책

- 네트워크 공유 경로가 올바르지 않는 경우 올바른 네트워크 공유 경로를 입력하십시오. IP 주소를 포함한 네트워크 공유 경로를 지원하지 않습니다.
- 네트워크 공유가 액세스할 수 없는 도메인에 위치한 경우 연결 서버 호스트에서 액세스할 수 있는 도메인의 네트워크 공유에 애플리케이션 패키지를 복사하십시오.

- 공유 폴더에 대한 파일 및 공유 사용 권한이 기본 Active Directory 그룹 도메인 컴퓨터에 읽기 액세스를 허용하는지 확인하십시오. 도메인 컨트롤러에 ThinApp을 할당하려면 파일 및 공유 사용 권한이 기본 Active Directory 그룹 도메인 컨트롤러에 읽기 액세스를 허용하는지도 확인하십시오. 사용 권한을 설정 또는 변경한 이후 네트워크 공유에 액세스할 수 있으려면 20분 정도 소요될 수 있습니다.

Horizon Administrator에 ThinApp 애플리케이션을 추가할 수 없음

Horizon Administrator에서 Horizon Administrator에 ThinApp 애플리케이션을 추가할 수 없습니다.

문제

Horizon Administrator에서 **새 ThinApp 검사**를 클릭하면 MSI 패키지를 사용할 수 없습니다.

원인

애플리케이션 패키지가 MSI 형식이 아니거나 연결 서버 호스트에서 네트워크 공유의 디렉토리에 액세스할 수 없습니다.

해결책

- 애플리케이션 저장소의 애플리케이션 패키지가 MSI 형식인지 확인하십시오.
- 네트워크 공유가 ThinApp 애플리케이션에 필요한 Horizon 7 요구 사항을 충족하는지 확인합니다. 자세한 내용은 [ThinApp 애플리케이션을 위한 Horizon 7 요구 사항](#)에 나와 있습니다.
- 네트워크 공유의 디렉토리에 적절한 사용 권한이 있는지 확인하십시오. 자세한 내용은 [애플리케이션 저장소를 등록할 수 없음](#)에 나와 있습니다.

애플리케이션 저장소를 검사할 때 연결 서버 디버그 로그 파일에 메시지가 나타납니다. 연결 서버 로그 파일은 연결 서버 호스트의 `drive:\Documents and Settings\All Users\Application Data\VMware\WDM\logs` 디렉토리에 있습니다.

ThinApp 템플릿을 할당할 수 없음

시스템 또는 데스크톱 풀에 ThinApp 템플릿을 할당할 수 없습니다.

문제

시스템 또는 데스크톱 풀에 ThinApp 템플릿을 할당하려고 하면 Horizon Administrator에서 할당 오류를 반환합니다.

원인

시스템 또는 데스크톱 풀에 이미 할당된 애플리케이션이 ThinApp 템플릿에 포함되어 있거나, 이전에 다른 설치 유형으로 해당 시스템 또는 데스크톱 풀에 ThinApp 템플릿을 할당했습니다.

해결책

시스템 또는 데스크톱 풀에 이미 할당된 ThinApp 애플리케이션이 템플릿에 포함되어 있는 경우, 해당 애플리케이션이 포함되지 않은 템플릿을 새로 생성하거나 기존 템플릿을 수정하여 애플리케이션을 제거하십시오. 새 템플릿 또는 수정된 템플릿을 시스템 또는 데스크톱 풀에 할당합니다.

ThinApp 애플리케이션의 설치 유형을 변경하려면 시스템 또는 데스크톱 풀에서 기존 애플리케이션 할당을 제거해야 합니다. ThinApp 애플리케이션이 제거되면 다른 설치 유형으로 시스템 또는 데스크톱 풀에 ThinApp 애플리케이션을 할당할 수 있습니다.

ThinApp 애플리케이션이 설치되어 있지 않음

Horizon Administrator가 ThinApp 애플리케이션을 설치할 수 없습니다.

문제

ThinApp 애플리케이션 설치 상태는 설치 보류 중 또는 설치 오류로 표시됩니다.

원인

이 문제의 일반적인 원인에는 다음 사항이 포함됩니다.

- ThinApp 애플리케이션을 설치할 시스템에 디스크 공간이 충분하지 않습니다.
- 연결 서버 호스트와 시스템 간 또는 연결 서버 호스트와 애플리케이션 저장소 간의 네트워크 연결이 끊어졌습니다.
- ThinApp 애플리케이션을 네트워크 공유에서 액세스할 수 없습니다.
- ThinApp 애플리케이션이 이전에 설치되었거나, 디렉토리 또는 파일이 시스템에 이미 존재합니다.

문제 원인에 대한 자세한 내용은 Horizon Agent 및 연결 서버 로그 파일을 참조할 수 있습니다.

Horizon Agent 로그 파일은 시스템의 `drive:\ProgramData\VMware\WDM\logs`에 있습니다.

연결 서버 로그 파일은 연결 서버 호스트의 `drive:\Documents and Settings\All Users\Application Data\VMware\WDM\logs` 디렉토리에 있습니다.

해결책

- 1 Horizon Administrator에서 **카탈로그 > ThinApp**을 선택합니다.
- 2 ThinApp 애플리케이션의 이름을 클릭합니다.
- 3 **시스템** 탭에서 시스템을 선택하고 **설치 재시도**를 클릭하여 ThinApp 애플리케이션을 다시 설치합니다.

ThinApp 애플리케이션이 제거되지 않음

Horizon Administrator가 ThinApp 애플리케이션을 제거할 수 없습니다.

문제

ThinApp 애플리케이션 설치 상태가 제거 오류로 표시됩니다.

원인

이 오류의 일반적인 원인에는 다음 사항이 포함됩니다.

- Horizon Administrator가 제거를 시도할 때 ThinApp 애플리케이션이 사용 중입니다.
- 연결 서버 호스트와 시스템 사이의 네트워크 연결이 끊어졌습니다.

문제 원인에 대한 자세한 내용은 Horizon Agent 및 연결 서버 로그 파일을 참조할 수 있습니다.

Horizon Agent 로그 파일은 Windows XP 시스템에서는 `drive:\Documents and Settings\All Users\Application Data\VMware\WDM\logs`에, Windows 7 시스템에서는 `drive:\ProgramData\VMware\WDM\logs`에 있습니다.

연결 서버 로그 파일은 연결 서버 호스트의 `drive:\Documents and Settings\All Users\Application Data\VMware\WDM\logs` 디렉토리에 있습니다.

해결책

- 1 Horizon Administrator에서 **카탈로그 > ThinApp**을 선택합니다.
- 2 ThinApp 애플리케이션의 이름을 클릭합니다.
- 3 **시스템** 탭을 클릭하고 시스템을 선택한 후 **제거 재시도**를 클릭하여 제거 작업을 다시 시도합니다.
- 4 제거 작업이 계속 실패할 경우 시스템에서 ThinApp 애플리케이션을 수동으로 제거한 후 **데스크톱의 애플리케이션 상태 제거**를 클릭합니다.

이 명령은 Horizon Administrator의 ThinApp 애플리케이션 할당을 지웁니다. 시스템에 있는 파일이나 설정은 제거되지 않습니다.

중요 이 명령은 시스템에서 ThinApp 애플리케이션을 수동으로 제거한 후에만 사용하십시오.

잘못된 MSI 패키지

Horizon Administrator는 애플리케이션 저장소에서 잘못된 MSI 패키지를 보고합니다.

문제

Horizon Administrator는 검사 작업을 진행하는 동안 잘못된 MSI 패키지를 보고합니다.

원인

이 문제의 일반적인 원인은 다음과 같습니다.

- MIS 파일이 손상되었습니다.
- ThinApp으로 MSI 파일이 생성되지 않았습니다.
- 지원되지 않은 ThinApp 버전으로 MIS 파일이 생성 또는 다시 패키징되었습니다. ThinApp 4.6 이상을 사용해야 합니다.

해결책

MSI 패키지 관련 문제 해결 방법은 ThinApp 사용자 설명서를 참조하십시오.

ThinApp 구성 예

ThinApp 구성 예는 애플리케이션 캡처 및 패키징으로 시작하여 설치 상태 확인으로 끝나는 일반적인 ThinApp 구성을 단계별로 수행하도록 합니다.

사전 요구 사항

이 예에서 단계 수행 방법에 대한 자세한 정보를 보려면 다음 항목을 참조하십시오.

- 애플리케이션 패키지 캡처 및 저장
- 시스템 및 데스크톱 풀에 ThinApp 애플리케이션 할당

절차

- 1 <http://www.vmware.com/products/thinapp>에서 ThinApp 소프트웨어를 다운로드하여 클린 컴퓨터에 설치하십시오.

Horizon 7에서는 ThinApp 버전 4.6 이상이 지원됩니다.
- 2 ThinApp **Setup Capture** 마법사를 사용하여 MSI 형식의 애플리케이션을 캡처하고 패키징합니다.
- 3 연결 서버 호스트와 원격 데스크톱 모두에 액세스할 수 있는 Active Directory 도메인에 속해 있는 컴퓨터에 공유 폴더를 생성하고, 공유 폴더에 파일 및 공유 사용 권한을 구성하여 내장 Active Directory 그룹 도메인 컴퓨터에 읽기 액세스를 제공합니다.

ThinApp 애플리케이션을 도메인 컨트롤러에 할당할 경우 내장 Active Directory 그룹 도메인 컨트롤러에 읽기 액세스를 제공합니다.
- 4 MSI 패키지를 공유 폴더에 복사합니다.
- 5 Horizon Administrator의 애플리케이션 저장소로 공유 폴더를 등록합니다.
- 6 Horizon Administrator에서 애플리케이션 저장소의 MSI 패키지를 스캔하고 선택한 ThinApp 애플리케이션을 Horizon Administrator에 추가합니다.
- 7 시스템 또는 데스크톱 풀에 ThinApp 애플리케이션을 할당할지 여부를 결정합니다.

시스템에 일반 이름 지정 규칙을 사용할 경우 시스템 할당을 사용하여, 해당 이름 지정 규칙을 사용하는 모든 시스템에 애플리케이션을 신속하게 배포할 수 있습니다. 부서 또는 사용자 유형별로 데스크톱 풀을 구성하면 데스크톱 풀 할당을 사용하여 특정 부서나 사용자에게 애플리케이션을 신속하게 배포할 수 있습니다.

- 8 Horizon Administrator에서 시스템 또는 데스크톱 풀에 할당할 ThinApp 애플리케이션을 선택하고 설치 방법을 지정합니다.

옵션	조치
스트리밍	시스템에 애플리케이션의 바로 가기를 설치합니다. 바로 가기는 저장소를 호스팅하는 네트워크 공유에 있는 애플리케이션을 가리킵니다. 애플리케이션을 실행하려면 사용자가 네트워크 공유에 액세스할 수 있어야 합니다.
전체	시스템의 로컬 파일 시스템에 전체 애플리케이션을 설치합니다.

- 9 Horizon Administrator에서 ThinApp 애플리케이션의 설치 상태를 확인합니다.

키오스크 모드에서 클라이언트 설정

Horizon 7에서 데스크톱에 대한 액세스 권한을 얻을 수 있는 무인 클라이언트를 설정할 수 있습니다.

키오스크 모드의 클라이언트는 쉘 클라이언트이거나 연결 서버 인스턴스에 연결하고 세션을 시작하기 위해 Horizon Client를 실행하는 잠긴 PC입니다. 최종 사용자는 게시된 데스크톱에서 일부 애플리케이션에 인증 정보를 제공해야 하지만 일반적으로 클라이언트 디바이스에 액세스하기 위해 로그인할 필요는 없습니다. 샘플 애플리케이션에는 의료 데이터 입력 워크스테이션, 항공사 체크인 스테이션, 고객 셀프 서비스 장소 및 공용 액세스의 정보 터미널이 포함됩니다.

데스크톱 애플리케이션이 보안 트랜잭션에 대해 인증 메커니즘을 구현하고 임의 변경 및 침해에서 물리적 네트워크를 보호하고 네트워크에 연결된 모든 디바이스를 신뢰할 수 있도록 보장해야 합니다.

키오스크 모드의 클라이언트는 원격 세션 및 위치 기반 인증에 대해 USB 디바이스의 자동 리디렉션과 같은 원격 액세스의 표준 기능을 지원합니다.

Horizon 7는 Horizon 7 4.5 이상의 Flexible Authentication 기능을 사용하여 최종 사용자가 아닌 키오스크 모드의 클라이언트 디바이스를 인증합니다. "custom-" 문자 또는 ADAM에서 정의한 대체 접두사 문자열로 시작하는 사용자 이름 또는 MAC 주소로 식별하는 클라이언트를 인증하도록 연결 서버 인스턴스를 구성할 수 있습니다. 자동으로 생성된 암호가 있는 클라이언트를 구성할 경우 암호를 지정하지 않고 디바이스에서 Horizon Client를 실행할 수 있습니다. 명시적 암호를 구성할 경우 이 암호를 Horizon Client에 지정해야 합니다. 일반적으로 스크립트에서 Horizon Client를 실행하고 암호가 일반 텍스트로 나타날 경우 권한이 없는 사용자가 스크립트를 읽을 수 없도록 예방 조치를 취해야 합니다.

키오스크 모드에서 클라이언트를 인증할 수 있도록 설정한 연결 서버 인스턴스만 "cm-" 문자 뒤에 MAC 주소로 이어지며 시작하거나, "custom-" 문자로 시작하거나, 사용자가 정의한 대체 문자열로 시작하는 계정에서 오는 연결을 허용할 수 있습니다. Horizon 7 4.5 이상의 Horizon Client에서는 이러한 형식의 사용자 이름을 수동으로 입력할 수 없습니다.

모범 사례로서, 전용 연결 서버 인스턴스를 사용해 키오스크 모드에서 클라이언트를 처리하고 Active Directory에서 이들 클라이언트 계정에 대한 전용 조직 단위 및 그룹을 생성하십시오. 이 사례는 시스템을 분할해 허가 받지 않은 침입에 대비할 뿐 아니라 클라이언트를 보다 쉽게 구성 및 관리하도록 지원합니다.

키오스크 모드에서 클라이언트 구성

키오스크 모드에서 클라이언트를 지원하도록 Active Directory와 Horizon 7을 구성하려면 몇 가지 작업을 순서대로 수행해야 합니다.

사전 요구 사항

구성 작업에 필요한 권한을 가지고 있는지 확인하십시오.

- 도메인의 사용자 및 그룹 계정을 변경할 수 있는 Active Directory의 **도메인 관리자** 또는 **계정 운영자** 자격 증명
- **관리자, 인벤토리 관리자** 또는 동등한 역할로 Horizon Administrator를 사용해 사용자 또는 그룹에 원격 데스크톱에 대한 권한 부여
- **관리자** 또는 동등한 역할로 vdmadmin 명령 실행

절차

1 키오스크 모드의 클라이언트를 위해 Active Directory 및 Horizon 7 클라이언트 준비

생성할 계정이 클라이언트 디바이스를 인증하도록 Active Directory를 구성해야 합니다. 또한 그룹을 생성할 때마다 클라이언트가 액세스하는 데스크톱 풀에 대한 권한을 해당 그룹에 부여해야 합니다. 또한 클라이언트가 사용하는 데스크톱 풀을 준비할 수 있습니다.

2 키오스크 모드에서 클라이언트의 기본값 설정

vdmadmin 명령을 사용하여 키오스크 모드에서 클라이언트의 Active Directory에 조직 단위, 암호 만료 및 그룹 구성원 자격의 기본값을 설정할 수 있습니다.

3 클라이언트 디바이스의 MAC 주소 표시

MAC 주소에 기반하는 클라이언트 계정을 생성하려는 경우 Horizon Client를 사용하여 클라이언트 디바이스의 MAC 주소를 검색할 수 있습니다.

4 키오스크 모드에서 클라이언트의 계정 추가

vdmadmin 명령을 사용해 연결 서버 그룹 구성에 클라이언트에 대한 계정을 추가할 수 있습니다. 클라이언트를 추가한 후에는 클라이언트 인증을 사용하도록 설정한 연결 서버 인스턴스에서 사용할 수 있습니다. 클라이언트 구성을 업데이트하거나 시스템에서 해당 계정을 제거할 수 있습니다.

5 키오스크 모드에서 클라이언트 인증을 사용하도록 설정

vdmadmin 명령을 사용하면 연결 서버 인스턴스를 통해 원격 데스크톱에 연결하려는 클라이언트의 인증을 사용하도록 설정할 수 있습니다.

6 키오스크 모드에서 클라이언트의 구성 확인

vdmadmin 명령을 사용하여 키오스크 모드의 클라이언트 및 해당 클라이언트를 인증하도록 구성된 연결 서버 인스턴스에 대한 정보를 표시할 수 있습니다.

7 키오스크 모드로 클라이언트에서 원격 데스크톱에 연결

명령줄에서 클라이언트를 실행하거나 스크립트를 사용해 클라이언트를 원격 세션에 연결할 수 있습니다.

키오스크 모드의 클라이언트를 위해 Active Directory 및 Horizon 7 클라이언트 준비

생성할 계정이 클라이언트 디바이스를 인증하도록 Active Directory를 구성해야 합니다. 또한 그룹을 생성할 때마다 클라이언트가 액세스하는 데스크톱 풀에 대한 권한을 해당 그룹에 부여해야 합니다. 또한 클라이언트가 사용하는 데스크톱 풀을 준비할 수 있습니다.

모범 사례로 개별 조직 단위 및 그룹을 생성하여 키오스크 모드의 클라이언트 관리 작업을 최소화합니다. 임의 그룹에 속하지 않은 클라이언트의 개별 계정을 추가할 수 있지만 이로 인해 소수의 클라이언트보다 많이 구성할 경우 큰 관리 오버헤드가 생성됩니다.

절차

- 1 Active Directory에서 개별 조직 단위 및 그룹을 생성하여 키오스크 모드에서 클라이언트와 함께 사용합니다.

그룹에 Windows 2000 이전 이름을 지정해야 합니다. 이 이름을 사용하여 vdmadmin 명령에 대해 그룹을 식별합니다.

- 2 게스트 가상 시스템의 이미지 또는 템플릿을 생성하십시오.

vCenter Server에서 관리하는 가상 시스템을 자동화된 풀의 템플릿, 연결된 클론 풀의 상위 항목 또는 수동 데스크톱 풀의 가상 시스템으로 사용할 수 있습니다. 게스트 운영 체제에 애플리케이션을 설치하고 구성할 수도 있습니다.

- 3 무인 상태일 때 클라이언트가 잠기지 않도록 게스트 운영 체제를 구성합니다.

Horizon 7에서는 키오스크 모드로 연결하는 클라이언트의 사전 로그인 메시지를 표시하지 않습니다. 화면 잠금을 해제하고 메시지를 표시할 이벤트가 필요한 경우 게스트 운영 체제에 적절한 애플리케이션을 구성할 수 있습니다.

- 4 Horizon Administrator에서 클라이언트가 사용할 데스크톱 풀을 생성하고 이 풀에 대해 그룹에 권한을 부여하십시오.

예를 들어, 부동 할당, 연결된 클론 데스크톱 풀을 클라이언트 애플리케이션의 요구 사항에 가장 적합하게 생성할 수 있습니다. 또한 하나 이상의 ThinApp 애플리케이션을 데스크톱 풀과 연결할 수 있습니다.

중요 두 개 이상의 데스크톱 풀에 대해 클라이언트 또는 그룹에 권한을 부여하지 마십시오. 이렇게 하면 Horizon 7는 클라이언트가 권한을 가진 풀에서 원격 데스크톱을 임의로 할당하고 경고 이벤트를 생성합니다.

- 5 클라이언트용 위치 기반 인쇄를 사용하도록 설정할 경우 AutoConnect Location-based Printing for VMware View Active Directory 그룹 정책 설정을 구성하십시오(컴퓨터 구성 아래 소프트웨어 설정 폴더의 Microsoft Group Policy Object Editor에 있음).

- 6 클라이언트의 원격 데스크톱을 최적화하고 보호하는 데 필요한 다른 정책을 구성합니다.

예를 들어, 원격 데스크톱을 시작하거나 디바이스를 연결할 때 로컬 USB 디바이스를 원격 데스크톱에 연결하는 정책을 재정의할 수 있습니다. 기본적으로 Windows용 Horizon Client는 키오스크 모드의 클라이언트에 이러한 정책을 사용하도록 설정합니다.

예제: 키오스크 모드의 클라이언트를 위해 Active Directory 준비

회사 인트라넷에는 MYORG 도메인이 있고 조직 단위에는 OU=myorg-ou, DC=myorg, DC=com 고유 이름이 있습니다. Active Directory에서 키오스크 모드의 클라이언트와 함께 사용할 OU=kiosk-ou, DC=myorg, DC=com 고유 이름 및 kc-grp 그룹을 사용하여 조직 단위 kiosk-ou를 생성합니다.

다음에 수행할 작업

클라이언트의 기본값을 설정하십시오.

키오스크 모드에서 클라이언트의 기본값 설정

vdmadmin 명령을 사용하여 키오스크 모드에서 클라이언트의 Active Directory에 조직 단위, 암호 만료 및 그룹 구성원 자격의 기본값을 설정할 수 있습니다.

클라이언트가 게시된 데스크톱에 연결할 때 사용할 연결 서버 인스턴스가 포함된 그룹의 연결 서버 인스턴스 중 하나에서 vdmadmin 명령을 실행해야 합니다.

암호 만료와 Active Directory 그룹 구성원에 대해 기본값을 구성하는 경우에는 그룹의 모든 연결 서버 인스턴스에서 이들 설정을 공유합니다.

절차

- ◆ 클라이언트의 기본값을 설정하십시오.

```
vdmadmin -Q -clientauth -setdefaults [-b authentication_arguments] [-ou DN] [ -expirepassword |
-noexpirepassword ] [-group group_name | -nogroup]
```

옵션	설명
-expirepassword	클라이언트 계정의 암호 만료 시간을 연결 서버 그룹과 동일하게 지정합니다. 그룹의 암호 만료 시간을 정의하지 않은 경우에는 암호가 만료되지 않습니다.
-group group_name	클라이언트 계정을 추가할 기본 그룹의 이름을 지정합니다. 그룹의 이름은 Active Directory에서 Windows 2000 이전 그룹 이름으로 지정해야 합니다.
-noexpirepassword	클라이언트 계정의 암호가 만료되지 않도록 지정합니다.
-nogroup	기본 그룹의 설정을 지웁니다.
-ou DN	클라이언트 계정이 추가될 기본 조직 단위의 고유 이름을 지정합니다. 예: OU=kiosk-ou,DC=myorg,DC=com
참고 명령을 사용하여 조직 단위의 구성을 변경할 수 없습니다.	

명령은 연결 서버 그룹의 클라이언트 기본값을 업데이트합니다.

예제: 키오스크 모드에서 클라이언트의 기본값 설정

클라이언트 그룹의 구성원, 암호 만료, 조직 단위에 대한 기본값을 설정하십시오.

```
vdmadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

다음에 수행할 작업

인증에 MAC 주소를 사용하는 클라이언트 디바이스의 MAC 주소를 찾아 내십시오.

클라이언트 디바이스의 MAC 주소 표시

MAC 주소에 기반하는 클라이언트 계정을 생성하려는 경우 Horizon Client를 사용하여 클라이언트 디바이스의 MAC 주소를 검색할 수 있습니다.

사전 요구 사항

클라이언트의 콘솔에 로그인하십시오.

절차

- ◆ MAC 주소를 표시하려면 플랫폼에 대해 적절한 명령을 입력하십시오.

옵션	조치
Windows	<p><code>C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -printEnvironmentInfo</code>를 입력합니다.</p> <p>클라이언트는 이전에 구성된 기본 연결 서버 인스턴스를 사용합니다. 기본값을 구성하지 않은 경우에는 클라이언트가 사용자에게 값을 묻습니다.</p> <p>IP 주소, MAC 주소, 클라이언트 디바이스의 시스템 이름을 표시하는 명령입니다.</p>
Linux	<p><code>vmware-view --printEnvironmentInfo -s <i>connection_server</i></code>를 입력하십시오.</p> <p>클라이언트가 데스크톱에 연결할 때 사용할 연결 서버 인스턴스의 IP 주소 또는 FQDN을 지정해야 합니다.</p> <p>IP 주소, MAC 주소, 시스템 이름, 도메인, 로그인한 모든 사용자 이름과 도메인, 클라이언트 디바이스의 시간대를 표시하는 명령입니다.</p>

다음에 수행할 작업

클라이언트 계정을 추가하십시오.

키오스크 모드에서 클라이언트의 계정 추가

vdadmin 명령을 사용해 연결 서버 그룹 구성에 클라이언트에 대한 계정을 추가할 수 있습니다. 클라이언트를 추가한 후에는 클라이언트 인증을 사용하도록 설정한 연결 서버 인스턴스에서 사용할 수 있습니다. 클라이언트 구성을 업데이트하거나 시스템에서 해당 계정을 제거할 수 있습니다.

클라이언트가 게시된 데스크톱에 연결할 때 사용할 연결 서버 인스턴스가 포함된 그룹의 연결 서버 인스턴스 중 하나에서 vdadmin 명령을 실행해야 합니다.

키오스크 모드에서 클라이언트를 추가하는 경우 Horizon 7이 Active Directory에 클라이언트의 사용자 계정을 생성합니다. 클라이언트 이름을 지정할 경우 "custom-"과 같은 인식된 접두사 문자열 또는 ADAM에서 정의한 대체 접두사 문자열로 시작하고 20자 미만이어야 합니다. 클라이언트 이름을 지정하지 않을 경우에는 클라이언트 디바이스용으로 지정된 MAC 주소를 사용해 Horizon 7에서 이름을 생성합니다. 예를 들어, MAC 주소가 00:10:db:ee:76:80인 경우 해당하는 계정 이름은 cm-00_10_db_ee_76_80입니다. 이러한 계정은 클라이언트를 인증할 수 있는 연결 서버 인스턴스에 서만 사용할 수 있습니다.

중요 지정한 이름을 두 개 이상의 클라이언트 디바이스에서 사용하지 마십시오. 향후 릴리스에서는 이 구성을 지원하지 않을 수 있습니다.

절차

- ◆ 클라이언트의 MAC 주소 또는 이름 및 도메인을 지정하려면 `-domain`과 `-clientid` 옵션을 사용해 `vdmadmin` 명령을 실행하십시오.

```
vdmadmin -Q -clientauth -add [-b authentication_arguments] -domain domain_name -clientid client_id [-password "password" | -genpassword] [-ou DN] [-expirepassword | -noexpirepassword] [-group group_name | -nogroup] [-description "description_text"]
```

옵션	설명
<code>-clientid client_id</code>	클라이언트 이름 또는 MAC 주소를 지정합니다.
<code>-description "description_text"</code>	클라이언트 디바이스 계정에 대한 설명을 Active Directory에 생성합니다.
<code>-domain domain_name</code>	클라이언트의 도메인을 지정합니다.
<code>-expirepassword</code>	클라이언트 계정의 암호 만료 시간을 연결 서버 그룹의 암호 만료 시간과 동일하게 지정합니다. View Connection Server 그룹의 암호 만료 시간을 정의하지 않은 경우에는 암호가 만료되지 않습니다.
<code>-genpassword</code>	클라이언트 계정에 대한 암호를 생성합니다. <code>-password</code> 또는 <code>-genpassword</code> 를 지정하지 않을 경우 기본으로 사용되는 동작입니다. 암호는 16자로 생성되고 대문자, 소문자, 기호, 숫자를 최소 하나 이상씩 포함하며 동일 문자를 반복 사용할 수 있습니다. 보안 수준이 높은 암호가 필요하다면 <code>-password</code> 옵션을 사용해 암호를 지정하십시오.
<code>-group group_name</code>	클라이언트 계정이 추가되는 그룹의 이름을 지정합니다. 그룹의 이름은 Active Directory에서 Windows 2000 이전 그룹 이름으로 지정해야 합니다. 이전에 기본 그룹을 설정한 경우에는 기본 그룹에 클라이언트 계정이 추가됩니다.
<code>-noexpirepassword</code>	클라이언트 계정 암호가 만료되지 않도록 지정합니다.
<code>-nogroup</code>	클라이언트 계정이 기본 그룹에 추가되지 않도록 지정합니다.
<code>-ou DN</code>	클라이언트 계정이 추가되는 조직 단위의 고유 이름을 지정합니다. 예: OU=kiosk-ou,DC=myorg,DC=com
<code>-password "password"</code>	클라이언트 계정에 대한 명시적 암호를 지정합니다.

Active Directory에서 특정 도메인과 그룹(있을 경우)의 클라이언트에 대한 사용자 계정을 생성하는 명령입니다.

예제:클라이언트의 계정 추가

그룹 `kc-grp`의 기본 설정을 사용해서 MAC 주소로 지정한 클라이언트 계정을 `MYORG` 도메인에 추가합니다.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

자동으로 생성된 암호를 사용해서 MAC 주소로 지정한 클라이언트 계정을 `MYORG` 도메인에 추가합니다.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword
```

명명된 클라이언트 계정을 추가하고 클라이언트에서 사용할 암호를 지정합니다.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

자동으로 생성된 암호를 사용해서 명명된 클라이언트 계정을 추가합니다.

```
vdmadmin -Q -clientauth -add -domain MYORG -clientid custom-Kiosk11 -genpassword -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Kiosk 11"
```

다음에 수행할 작업

클라이언트 인증을 사용하도록 설정합니다.

키오스크 모드에서 클라이언트 인증을 사용하도록 설정

vdmadmin 명령을 사용하면 연결 서버 인스턴스를 통해 원격 데스크톱에 연결하려는 클라이언트의 인증을 사용하도록 설정할 수 있습니다.

클라이언트가 원격 데스크톱에 연결할 때 사용할 View 연결 서버 인스턴스가 포함된 그룹의 연결 서버 인스턴스 중 하나에서 vdmadmin 명령을 실행해야 합니다.

개별 연결 서버 인스턴스에 대한 인증을 사용하도록 설정해도 그룹에 있는 모든 연결 서버 인스턴스에서 클라이언트 인증에 대한 다른 설정을 모두 공유합니다. 클라이언트 계정을 한 번만 추가하면 됩니다. 연결 서버 그룹에서 활성화된 연결 서버 인스턴스는 모두 클라이언트를 인증할 수 있습니다.

RDS 호스트에서 세션 기반 데스크톱과 함께 키오스크 모드를 사용하려면 사용자 계정을 원격 데스크톱 사용자 그룹에 추가해야 합니다.

절차

- 1 연결 서버 인스턴스에서 클라이언트 인증을 사용하도록 설정하십시오.

```
vdmadmin -Q -enable [-b authentication_arguments] -s connection_server [-requirepassword]
```

옵션	설명
-requirepassword	클라이언트에서 암호를 입력하도록 지정합니다. 중요 이 옵션을 지정하면 연결 서버 인스턴스에서 암호가 자동 생성된 클라이언트를 인증할 수 없습니다. 연결 서버 인스턴스 구성을 변경해 이 옵션을 지정하면 이러한 클라이언트는 자신을 인증할 수 없어 인증이 실패하고 알 수 없는 사용자 이름 또는 잘못된 암호라는 오류 메시지가 표시됩니다.
-s connection_server	클라이언트 인증을 사용하도록 설정할 연결 서버 인스턴스의 NetBIOS 이름을 지정합니다.

이 명령으로 지정된 연결 서버 인스턴스에서 클라이언트를 인증하도록 설정할 수 있습니다.

2. 게시된 데스크톱이 Microsoft RDS 호스트에서 제공되는 경우 RDS 호스트에 로그인한 후 사용자 계정을 원격 데스크톱 사용자 그룹에 추가합니다.

예를 들어 Horizon 7 Server에서 custom-11 사용자 계정을 RDS 호스트의 세션 기반 데스크톱에 부여한다고 가정해 봅시다. 그러면 RDS 호스트에 로그인하고 **제어판 > 시스템 및 보안 > 시스템 > 원격 설정 > 사용자 선택 > 추가**로 이동하여 custom-11 사용자를 원격 데스크톱 사용자 그룹에 추가해야 합니다.

예제: 키오스크 모드에서 클라이언트 인증을 사용하도록 설정

연결 서버 인스턴스 csvr-2에 대한 클라이언트 인증을 사용하도록 설정합니다. 자동 생성된 암호를 갖는 클라이언트는 암호를 제공하지 않고 자신을 인증할 수 있습니다.

```
vdadmin -Q -enable -s csvr-2
```

연결 서버 인스턴스 csvr-3에 대한 클라이언트 인증을 사용하도록 설정하고 클라이언트가 Horizon Client에 대한 자신의 암호를 지정하도록 요구합니다. 암호가 자동 생성된 클라이언트는 자신을 인증할 수 없습니다.

```
vdadmin -Q -enable -s csvr-3 -requirepassword
```

다음에 수행할 작업

연결 서버 인스턴스 및 클라이언트 구성을 확인하십시오.

키오스크 모드에서 클라이언트의 구성 확인

vdadmin 명령을 사용하여 키오스크 모드의 클라이언트 및 해당 클라이언트를 인증하도록 구성된 연결 서버 인스턴스에 대한 정보를 표시할 수 있습니다.

클라이언트가 원격 데스크톱에 연결할 때 사용할 View 연결 서버 인스턴스가 포함된 그룹의 연결 서버 인스턴스 중 하나에서 vdadmin 명령을 실행해야 합니다.

절차

- ◆ 키오스크 모드의 클라이언트 및 클라이언트 인증에 대한 정보를 표시합니다.

```
vdadmin -Q -clientauth -list [-b authentication_arguments] [-xml]
```

이 명령은 클라이언트 인증을 사용하도록 설정한 연결 서버 인스턴스 및 키오스크 모드의 클라이언트에 대한 정보를 표시합니다.

예제: 키오스크 모드에서 클라이언트의 정보 표시

텍스트 형식으로 클라이언트에 대한 정보를 표시합니다. 클라이언트 cm-00_0c_29_0d_a3_e6의 암호는 자동으로 생성되었기 때문에 Horizon Client에 최종 사용자가 암호를 입력하거나 애플리케이션 스크립트를 통해 암호를 지정할 필요가 없습니다. 클라이언트 cm-00_22_19_12_6d_cf의 암호는 명시적으로 지정되었으며 최종 사용자가 이 암호를 입력해야 합니다. 연결 서버 인스턴스 CONSVR2는 암호가 자동 생성된 클라이언트의 인증 요청을 허용합니다. CONSVR1은 키오스크 모드에서 클라이언트의 인증 요청을 허용하지 않습니다.

```
C:\W vdmadmin -Q -clientauth -list
Client Authentication User List
=====
GUID                : 94be6344-0c9b-4a92-8d54-1brc1c2dc282
ClientID            : cm-00_0c_29_0d_a3_e6
Domain              : myorg.com
Password Generated: true

GUID                : 471d9d35-68b2-40ee-b693-56a7d92b2e25
ClientID            : cm-00_22_19_12_6d_cf
Domain              : myorg.com
Password Generated: false

Client Authentication Connection Servers
=====
Common Name          : CONSVR1
Client Authentication Enabled : false
Password Required    : false

Common Name          : CONSVR2
Client Authentication Enabled : true
Password Required    : false
```

다음에 수행할 작업

클라이언트가 해당 원격 데스크톱에 연결할 수 있는지 확인합니다.

키오스크 모드로 클라이언트에서 원격 데스크톱에 연결

명령줄에서 클라이언트를 실행하거나 스크립트를 사용해 클라이언트를 원격 세션에 연결할 수 있습니다.

배포된 클라이언트 디바이스에서 Horizon Client를 실행하려면 일반적으로 명령 스크립트를 사용합니다.

참고 Windows 또는 Mac 클라이언트에서는 원격 데스크톱 세션이 시작될 때 다른 애플리케이션 또는 서비스에서 클라이언트의 USB 디바이스를 사용하는 경우 기본적으로 해당 디바이스는 자동으로 전달되지 않습니다. 모든 클라이언트에서 휴먼 인터페이스 디바이스(HID) 및 스마트 카드 판독기가 기본적으로 전달되지 않습니다.

절차

- ◆ 원격 세션에 연결하려면 플랫폼에 적절한 명령을 입력하십시오.

옵션	설명
Windows	<p>C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended [-serverURL <i>connection_server</i>] [-userName <i>user_name</i>] [-password <i>password</i>]를 입력합니다.</p> <p>-password password 클라이언트 계정에 대한 암호를 지정합니다. 계정에 대한 암호를 정의한 경우 이 암호를 지정해야 합니다.</p> <p>-serverURL connection_server Horizon Client가 원격 데스크톱에 연결할 때 사용할 연결 서버 인스턴스의 IP 주소 또는 FQDN을 지정합니다. 클라이언트가 원격 데스크톱에 연결할 때 사용할 연결 서버 인스턴스의 IP 주소 또는 FQDN을 지정하지 않은 경우 클라이언트는 구성해 놓은 기본 연결 서버 인스턴스를 사용합니다.</p> <p>-userName user_name 클라이언트 계정의 이름을 지정합니다. 클라이언트에서 MAC 주소가 아닌 "custom-"과 같은 인식된 접두사 문자열로 시작하는 계정 이름을 사용해 자신을 검증하도록 구성하려면 이 이름을 지정해야 합니다.</p>
Linux	<p>vmware-view --unattended -s <i>connection_server</i> [--once] [-u <i>user_name</i>] [-p <i>password</i>]를 입력하십시오.</p> <p>--once 오류 발생 시 Horizon Client에서 다시 연결을 시도하지 않도록 지정합니다.</p> <p>중요 일반적으로 이 옵션을 지정하고 종료 코드를 사용해 오류를 처리해야 합니다. 그렇지 않으면 원격으로 vmware-view 프로세스를 중지하기 어려울 수 있습니다.</p> <p>-p password 클라이언트 계정에 대한 암호를 지정합니다. 계정에 대한 암호를 정의한 경우 이 암호를 지정해야 합니다.</p> <p>-s connection_server 클라이언트가 데스크톱에 연결할 때 사용할 연결 서버 인스턴스의 IP 주소 또는 FQDN을 지정합니다.</p> <p>-u user_name 클라이언트 계정의 이름을 지정합니다. 클라이언트에서 MAC 주소가 아닌 "custom-"과 같은 인식된 접두사 문자열로 시작하는 계정 이름을 사용해 자신을 검증하도록 구성하려면 이 이름을 지정해야 합니다.</p>

서버가 키오스크 클라이언트를 인증하고 원격 데스크톱을 사용할 수 있는 경우 원격 세션을 시작하는 명령입니다.

예제: 키오스크 모드로 클라이언트에서 Horizon Client 실행

계정 이름이 MAC 주소에 기반하고 암호가 자동으로 생성된 Windows 클라이언트에서 Horizon Client를 실행합니다.

```
C:\Program Files (x86)\VMware\VMware Horizon View Client\vmware-view.exe -unattended -serverURL consvr2.myorg.com
```

할당된 이름 및 암호를 사용해 Linux 클라이언트에서 Horizon Client를 실행합니다.

```
vmware-view -unattended -s 145.124.24.100 --once -u custom-Terminal21 -p "Secret1!"
```

Horizon 7 문제 해결

Horizon 7를 사용할 때 발생할 수 있는 문제에 대해 다양한 진단 및 해결 절차를 사용할 수 있습니다. 문제 해결을 위해 Horizon Help Desk Tool을 사용하고, 다른 문제 해결 절차를 사용하여 문제를 조사 및 수정하거나, VMware 기술 지원에서 지원을 얻을 수 있습니다.

데스크톱 및 데스크톱 풀 문제 해결에 대한 자세한 내용은 Horizon 7에서 가상 데스크톱 설정 문서를 참조하십시오.

본 장은 다음 항목을 포함합니다.

- [Horizon Help Desk Tool 사용](#)
- [VMware Logon Monitor 사용](#)
- [VMware Horizon 성능 추적기 사용](#)
- 시스템 상태 모니터링
- [Horizon 7의 이벤트 모니터링](#)
- [Horizon 7의 진단 정보 수집](#)
- 지원 요청 업데이트
- 보안 서버와 Horizon 연결 서버와의 연결 실패 문제 해결
- [Horizon 7 Server 인증서 해지 검사 문제 해결](#)
- [스마트 카드 인증서 해지 검사 문제 해결](#)
- 문제 해결 추가 정보

Horizon Help Desk Tool 사용

Horizon Help Desk Tool은 Horizon 7 사용자 세션 상태를 가져오고 문제 해결 및 유지 보수 작업을 수행하는 데 사용할 수 있는 웹 애플리케이션입니다.

Horizon Help Desk Tool에서 사용자 세션을 조회하여 문제를 해결하고 데스크톱 다시 시작 또는 재설정과 같은 데스크톱 유지 보수 작업을 수행할 수 있습니다.

Horizon Help Desk Tool을 구성하려면 다음 요구 사항을 충족해야 합니다.

- Horizon 7에 대한 Horizon Enterprise Edition 라이선스 또는 Horizon Apps Advanced Edition 라이선스. 올바른 라이선스가 있는지 확인하려면 [Horizon Help Desk Tool 라이선스 확인](#)을 참조하십시오.

- Horizon 7 구성 요소에 대한 정보를 저장하는 이벤트 데이터베이스. 이벤트 데이터베이스 구성에 대한 자세한 내용은 Horizon 7 설치 문서를 참조하십시오.
- Horizon Help Desk Tool에 로그인하기 위한 헬프 데스크 관리자 역할 또는 헬프 데스크 관리자 (읽기 전용) 역할. 이러한 역할에 대한 자세한 내용은 [Horizon Help Desk Tool에 대한 역할 기반 액세스 구성](#)을 참조하십시오.
- 로그인 세그먼트를 보려면 각 연결 서버 인스턴스에서 타이밍 프로파일러를 사용하도록 설정합니다.

각 연결 서버 인스턴스에서 타이밍 프로파일러를 사용하도록 설정하려면 다음 vdmadmin 명령을 사용합니다.

```
vdmadmin -l -timingProfiler -enable
```

관리 포트를 사용하는 연결 서버 인스턴스에서 타이밍 프로파일러를 사용하도록 설정하려면 다음 vdmadmin 명령을 사용합니다.

```
vdmadmin -l -timingProfiler -enable -server {ip/server}
```

Horizon Help Desk Tool 라이선스 확인

유효한 제품 라이선스 키가 없는 경우 Horizon Help Desk Tool에 로그인할 수 없습니다. Horizon Administrator에서 제품 라이선스 키를 확인하고 유효한 라이선스를 적용할 수 있습니다.

사전 요구 사항

- Horizon Enterprise Edition 라이선스 또는 Horizon Apps Advanced Edition 라이선스에 대한 유효한 제품 라이선스 키를 가져옵니다.

절차

- 1 Horizon Administrator에서 **View 구성 > 제품 라이선싱 및 사용량**을 선택합니다.

현재 라이선스 키의 처음과 마지막 다섯 자가 **라이선싱** 패널에 표시됩니다.

- 2 **헬프 데스크 라이선스** 필드의 라이선스 상태를 확인합니다.

옵션	설명
사용 안 함	제품 라이선스 키가 유효하지 않습니다. Horizon Help Desk Tool에 로그인할 수 없습니다.
사용	제품 라이선스 키가 유효합니다. Horizon Help Desk Tool에 로그인할 수 있습니다.

- 3 (선택 사항) 제품 라이선스 키를 유효하지 않으면 **라이선스 편집**을 클릭하고 유효한 라이선스 일련 번호를 입력한 후 **확인**을 클릭하고 Horizon Administrator URL을 새로 고칩니다.

제품 라이선싱 창에 업데이트된 라이선싱 정보가 표시됩니다.

다음에 수행할 작업

Horizon Help Desk Tool에 로그인합니다.

Horizon Help Desk Tool 에 대한 역할 기반 액세스 구성

Horizon Help Desk Tool 관리자에게 미리 정의된 관리자 역할을 할당하여 관리자 사용자 간에 문제 해결 작업을 위임할 수 있습니다. 또한 사용자 지정 역할을 생성하고, 미리 정의된 관리자 역할에 따라 권한을 추가할 수 있습니다.

Horizon Help Desk Tool 관리자에게 다음과 같은 미리 정의된 관리자 역할을 할당할 수 있습니다.

- 헬프 데스크 관리자
- 헬프 데스크 관리자(읽기 전용)

Horizon Help Desk Tool 관리자에 대해 사용자 지정 역할을 생성하는 경우 헬프 데스크 관리자 역할 또는 헬프 데스크 관리자(읽기 전용) 역할을 기준으로 다른 권한을 할당할 때 헬프 데스크 관리(읽기 전용) 권한을 할당해야 합니다.

사전 요구 사항

사용자 지정 역할 생성 시 사용할 수 있는 관리자 권한을 숙지하십시오. [미리 정의된 역할 및 권한](#) 항목을 참조하십시오.

절차

- 1 Horizon Administrator에서 **View 구성 > 관리자**를 선택하고 **역할** 탭을 클릭합니다.
- 2 **역할** 탭에서 **역할 추가**를 클릭하고 헬프 데스크 관리자 역할 또는 헬프 데스크 관리자(읽기 전용) 역할을 선택한 후 **확인**을 클릭합니다.
 - a (선택 사항) 사용자 지정 역할을 추가하려면 **역할** 탭에서 **역할 추가**를 클릭하고 [헬프 데스크 관리(읽기 전용)] 권한을 선택한 후 헬프 데스크 관리자 역할 또는 헬프 데스크 관리자(읽기 전용) 역할에 따라 권한을 선택하고 **확인**을 클릭합니다.

Horizon Help Desk Tool 에 로그인

Horizon Help Desk Tool이 Horizon Console에 통합되었습니다. Horizon 7 버전 7.5부터 더 이상 Horizon Help Desk Tool URL을 사용하여 Horizon Help Desk Tool에 로그인할 수 없습니다.

절차

- 1 Horizon Administrator에서 Horizon Help Desk Tool에 로그인하려면 오른쪽 상단 패널에서 **Horizon Console**을 클릭합니다. 이것은 Horizon Console 웹 인터페이스에 대한 Single Sign-On입니다.
- 2 Horizon Console에서 [사용자 검색] 필드에 사용자 이름을 입력합니다.
Horizon Console의 검색 결과에 사용자 목록이 표시됩니다. 검색 시 최대 100개의 일치하는 결과가 반환될 수 있습니다.
- 3 사용자 이름을 선택합니다.
사용자 정보가 사용자 카드에 표시됩니다.

다음에 수행할 작업

문제를 해결하려면 사용자 카드에서 관련 탭을 클릭합니다.

Horizon Help Desk Tool 에서 사용자 문제 해결

Horizon Help Desk Tool에서는 사용자 카드의 기본 사용자 정보를 볼 수 있습니다. 사용자 카드에서 탭을 클릭하여 특정 구성 요소에 대한 자세한 정보를 얻을 수 있습니다.

경우에 따라 사용자 세부 정보가 표에 제공될 수도 있습니다. 표 열을 기준으로 이러한 사용자 세부 정보를 정렬할 수 있습니다.

- 열을 오름차순으로 정렬하려면 열을 한 번 클릭합니다.
- 열을 내림차순으로 정렬하려면 열을 두 번 클릭합니다.
- 열을 정렬하지 않으려면 열을 세 번 클릭합니다.

기본 사용자 정보

사용자의 사용자 이름, 전화 번호 및 이메일 주소와 같은 기본 사용자 정보와 사용자의 연결 또는 연결 해제 상태를 표시합니다. 사용자에게 데스크톱 또는 애플리케이션 세션이 있는 경우 사용자는 연결된 상태입니다. 사용자에게 데스크톱 또는 애플리케이션 세션이 없는 경우 사용자는 연결 해제된 상태입니다.

전화 번호를 클릭하여 비즈니스용 Skype 세션을 열고 문제 해결 작업을 사용자와 협력하기 위해 해당 사용자에게 연락할 수 있습니다.

이메일을 클릭하여 사용자에게 메시지를 전송할 수도 있습니다.

세션

세션 탭에는 사용자가 연결되는 데스크톱 또는 애플리케이션 세션에 대한 정보가 표시됩니다.

필터 텍스트 상자를 사용하여 데스크톱 또는 애플리케이션 세션을 필터링할 수 있습니다.

참고 세션 탭에는 Microsoft RDP 디스플레이 프로토콜을 사용하는 세션 또는 vSphere Client 또는 ESXi에서 VM에 액세스하는 세션에 대한 세션 정보는 표시되지 않습니다.

세션 탭에는 다음 정보가 포함됩니다.

표 11-1. 세션 탭

옵션	설명
상태	<p>데스크톱 또는 애플리케이션 세션의 상태에 대한 정보를 표시합니다.</p> <ul style="list-style-type: none"> ■ 세션이 연결된 경우 녹색으로 나타납니다. ■ L: 세션이 로컬 세션이거나 로컬 포트에서 실행되는 세션인 경우. ■ G: 세션이 포트 페더레이션의 다른 포트에서 실행되는 경우.
컴퓨터 이름	<p>데스크톱 또는 애플리케이션 세션의 이름입니다. 이름을 클릭하여 카드의 세션 정보를 엽니다.</p> <p>세션 카드에 있는 탭을 클릭하여 추가 정보를 볼 수 있습니다.</p> <ul style="list-style-type: none"> ■ 세부 정보 탭에는 VM 정보, CPU 또는 메모리 사용량 같은 사용자 정보가 표시됩니다. Horizon Help Desk Tool에 대한 세션 세부 정보를 참조하십시오. ■ 프로세스 탭에는 CPU 및 메모리 관련 프로세스에 대한 정보가 표시됩니다. Horizon Help Desk Tool에 대한 세션 프로세스를 참조하십시오. ■ 애플리케이션 탭에는 실행 중인 애플리케이션에 대한 세부 정보가 표시됩니다. Horizon Help Desk Tool에 대한 애플리케이션 상태를 참조하십시오.
프로토콜	데스크톱 또는 애플리케이션 세션에 대한 디스플레이 프로토콜입니다.
유형	데스크톱이 게시된 데스크톱인지, 가상 시스템 데스크톱인지 또는 애플리케이션인지를 표시합니다.
연결 시간	연결 서버에 세션이 연결된 시간입니다.
세션 기간	세션이 연결 서버와 연결된 상태를 유지하는 기간입니다.

데스크톱 권한

데스크톱 사용 권한 탭에는 사용자에게 사용 권한이 부여된, 게시된 데스크톱 또는 가상 데스크톱에 대한 정보가 표시됩니다.

표 11-2. 데스크톱 권한

옵션	설명
상태	<p>데스크톱 세션의 상태에 대한 정보를 표시합니다.</p> <ul style="list-style-type: none"> ■ 세션이 연결된 경우 녹색으로 나타납니다.
데스크톱 풀 이름	세션의 데스크톱 풀 이름입니다.
데스크톱 유형	데스크톱이 게시된 데스크톱인지 또는 가상 시스템 데스크톱인지를 표시합니다.
	<p>참고 세션이 포트 페더레이션의 다른 포트에서 실행되는 경우 어떤 정보도 표시되지 않습니다.</p>
유형	<p>데스크톱 권한 유형에 대한 정보를 표시합니다.</p> <ul style="list-style-type: none"> ■ 로컬: 로컬 권한의 경우 ■ 전역: 전역 권한의 경우

표 11-2. 데스크톱 권한 (계속)

옵션	설명
vCenter	vCenter Server에 있는 가상 시스템 이름을 표시합니다. 참고 세션이 포드 페더레이션의 다른 포드에서 실행되는 경우 어떤 정보도 표시되지 않습니다.
기본 프로토콜	데스크톱 또는 애플리케이션 세션에 대한 기본 디스플레이 프로토콜입니다.

애플리케이션 권한

애플리케이션 권한 탭에는 사용자에게 사용 권한이 부여된, 게시된 애플리케이션에 대한 정보가 표시됩니다.

표 11-3. 애플리케이션 권한

옵션	설명
상태	애플리케이션 세션의 상태에 대한 정보를 표시합니다. ■ 세션이 연결된 경우 녹색으로 나타납니다.
애플리케이션	애플리케이션 풀에서 게시된 애플리케이션의 이름을 표시합니다.
팜	세션이 연결되는 RDS 호스트를 포함하는 팜의 이름입니다. 참고 전역 애플리케이션 사용 권한의 경우 이 열에는 전역 애플리케이션 사용 권한의 팜 수가 표시됩니다.
유형	애플리케이션 권한 유형에 대한 정보를 표시합니다. ■ 로컬: 로컬 권한의 경우 ■ 전역: 전역 권한의 경우
게시자	게시된 애플리케이션의 소프트웨어 제조업체 이름입니다.

활동

활동 탭에는 사용자 활동에 대한 이벤트 로그 정보가 표시됩니다. 최근 12시간, 최근 30일 같은 시간 범위 또는 관리자 이름을 기준으로 활동을 필터링할 수 있습니다. Horizon Help Desk Tool 활동만을 기준으로 필터링하려면 **기술 지원 이벤트만 해당**을 클릭합니다. 새로 고침 아이콘을 클릭하여 이벤트 로그를 새로 고칩니다. 이벤트 로그를 파일로 내보내려면 내보내기 아이콘을 클릭합니다.

참고 CPA 환경의 사용자에게 대해서는 이벤트 로그 정보가 표시되지 않습니다.

표 11-4. 활동

옵션	설명
시간	시간 범위를 선택합니다. 기본값은 최근 12시간입니다. <ul style="list-style-type: none"> ■ 최근 12시간 ■ 최근 24시간 ■ 최근 7일 ■ 최근 30일 ■ 모두
관리자	관리자 사용자의 이름입니다.
메시지	사용자 또는 관리자가 수행한 활동에 국한되는 사용자 또는 관리자에 대한 메시지를 표시합니다.
리소스 이름	활동이 수행된 데스크톱 풀 또는 가상 시스템 이름에 대한 정보를 표시합니다.

Horizon Help Desk Tool 에 대한 세션 세부 정보

세션 사용자 세부 정보는 **세션** 탭에서 **컴퓨터 이름** 옵션에 있는 사용자 이름을 클릭하면 **세부 정보** 탭에 나타납니다. Horizon Client, 가상 또는 게시된 데스크톱에 대한 세부 정보와 CPU 및 메모리 세부 정보를 볼 수 있습니다.

Horizon Client

Horizon Client 유형에 따라 정보를 표시하고 사용자 이름, Horizon Client 버전, 클라이언트 시스템의 IP 주소 및 클라이언트 시스템의 운영 체제와 같은 세부 정보를 포함합니다.

참고 Horizon Agent를 업그레이드한 경우 Horizon Client도 최신 버전으로 업그레이드해야 합니다. 그렇지 않으면 Horizon Client에 대한 버전이 표시되지 않습니다. Horizon Client 업그레이드에 대한 자세한 내용은 Horizon 7 업그레이드 문서를 참조하십시오.

VM

가상 데스크톱 또는 게시된 데스크톱에 대한 정보를 표시합니다.

표 11-5. VM 세부 정보

옵션	설명
컴퓨터 이름	데스크톱 또는 애플리케이션 세션의 이름입니다.
에이전트 버전	Horizon Agent 버전입니다.
세션 상태	데스크톱 또는 애플리케이션 세션의 상태입니다.
상태 기간	세션이 동일한 상태를 유지하는 시간입니다.
로그온 시간	세션에 로그인한 사용자의 로그인 시간입니다.
로그온 기간	사용자가 세션에 로그인된 상태를 유지하는 시간입니다.
세션 기간	세션이 연결 서버에 연결된 상태를 유지하는 시간입니다.
연결 서버	세션이 연결된 연결 서버입니다.

표 11-5. VM 세부 정보 (계속)

옵션	설명
Unified Access Gateway 이름	Unified Access Gateway 장치의 이름입니다. 이 정보는 세션에 연결한 후 30초~60초 후에 표시될 수 있습니다.
Unified Access Gateway IP	Unified Access Gateway 장치의 IP 주소입니다. 이 정보는 세션에 연결한 후 30초~60초 후에 표시될 수 있습니다.
풀	데스크톱 또는 애플리케이션 풀의 이름입니다.
팜	게시된 데스크톱 또는 애플리케이션 세션의 RDS 호스트 팜입니다.
vCenter	vCenter Server의 IP 주소입니다.

Blast 메트릭 표시

VMware Blast 디스플레이 프로토콜을 사용하는 가상 또는 게시된 데스크톱 세션에 대한 성능 세부 정보를 표시합니다. 이러한 성능 세부 정보를 보려면 **Blast 메트릭 표시**를 클릭합니다.

표 11-6. Blast 디스플레이 프로토콜 세부 정보

옵션	설명
Blast 세션 카운터	<ul style="list-style-type: none"> ■ 예상 대역폭(업링크). 업링크 신호의 예상 대역폭입니다. ■ 패킷 손실(업링크). 업링크 신호의 패킷 손실 백분율입니다.
Blast 이미징 카운터	<ul style="list-style-type: none"> ■ 전송된 바이트. Blast 세션에 대해 전송된 이미징 데이터의 총 바이트 수입니다. ■ 수신된 바이트. Blast 세션에 대해 수신된 이미징 데이터의 총 바이트 수입니다.
Blast 오디오 카운터	<ul style="list-style-type: none"> ■ 전송된 바이트. Blast 세션에 대해 전송된 오디오 데이터의 총 바이트 수입니다. ■ 수신된 바이트. Blast 세션에 대해 수신된 오디오 데이터의 총 바이트 수입니다.
Blast CDR 카운터	<ul style="list-style-type: none"> ■ 전송된 바이트. Blast 세션에 대해 전송된 클라이언트 드라이브 리디렉션 데이터의 총 바이트 수입니다. ■ 수신된 바이트. Blast 세션에 대해 수신된 클라이언트 드라이브 리디렉션 데이터의 총 바이트 수입니다.

CPU, 메모리 및 지연 시간

가상 또는 게시된 데스크톱 또는 애플리케이션의 CPU 및 메모리 사용량과 PCoIP 또는 Blast 디스플레이 프로토콜에 대한 지연 시간을 차트로 표시합니다.

표 11-7. CPU, 메모리 및 지연 시간 세부 정보

옵션	설명
세션 CPU	현재 세션의 CPU 사용량입니다.
호스트 CPU	세션이 할당된 가상 시스템의 CPU 사용량입니다.
세션 메모리	현재 세션의 메모리 사용량입니다.

표 11-7. CPU, 메모리 및 지연 시간 세부 정보 (계속)

옵션	설명
호스트 메모리	세션이 할당된 가상 시스템의 메모리 사용량입니다.
세션 지연 시간	PCoIP 또는 Blast 디스플레이 프로토콜의 지연 시간 차트를 표시합니다. Blast 디스플레이 프로토콜의 경우 지연 시간은 왕복 시간(밀리초)입니다. 이 지연 시간을 추적하는 성능 카운터는 VMware Blast 세션 카운터 > RTT 입니다. PCoIP 디스플레이 프로토콜의 경우 지연 시간은 왕복 지연 시간(밀리초)입니다. 이 지연 시간을 추적하는 성능 카운터는 PCoIP 세션 네트워크 통계 > 왕복 지연 시간 입니다.

세션 로그인 세그먼트

로그온 동안 생성된 로그인 기간 및 사용량 세그먼트를 표시합니다.

표 11-8. 세션 로그인 세그먼트

옵션	설명
로그온 기간	사용자가 데스크톱 또는 애플리케이션 풀을 클릭한 시간부터 Windows 탐색기가 시작된 시간까지 계산된 기간입니다.
세션 로그인 시간	사용자가 세션에 로그인된 기간입니다.
로그온 세그먼트	로그온 동안 생성된 세그먼트를 표시합니다. <ul style="list-style-type: none"> ■ 브로커링. 연결 서버에서 세션 연결 또는 다시 연결을 처리하는 총 시간. 사용자가 데스크톱 풀을 클릭하는 시간부터 터널 연결이 설정되는 시간까지 계산됩니다. 사용자 인증, 시스템 선택 및 터널 연결 설정을 위한 시스템 준비 등의 연결 서버 작업 시간이 포함됩니다. ■ GPO 로드. Windows 그룹 정책 처리의 총 시간. 전역 정책이 구성되지 않은 경우 0을 표시합니다. ■ 프로파일 로드. Windows 사용자 프로파일 처리의 총 시간. ■ 대화형. Horizon Agent에서 세션 연결 또는 다시 연결을 처리하는 총 시간. PCoIP 또는 Blast Extreme이 터널 연결을 사용하는 시간부터 Windows 탐색기가 시작된 시간까지 계산됩니다. ■ 인증. 연결 서버에서 세션을 인증하는 데 소요되는 총 시간입니다. ■ VM 시작. VM을 시작하는 데 소요된 총 시간입니다. 이 시간에는 운영 체제 부팅, 일시 중단된 시스템 재개에 소요되는 시간과 Horizon Agent가 연결 준비가 완료되었음을 신호로 알리는 데 걸리는 시간이 포함됩니다.

문제 해결을 위해 로그인 세그먼트의 정보를 사용할 때 다음 지침을 사용합니다.

- 세션이 새 가상 데스크톱 세션인 경우 모든 로그인 세그먼트가 나타납니다. 전역 정책이 구성되지 않은 경우 **GPO 로드** 로그인 세그먼트 시간이 0입니다.
- 가상 데스크톱 세션이 연결 해제된 세션에서 다시 연결된 세션인 경우 **로그온 기간**, **대화형** 및 **브로커링** 로그인 세그먼트가 나타납니다.

- 세그먼트가 게시된 데스크톱 세션인 경우 **로그온 시간**, **GPO 로드** 또는 **프로파일 로드** 로그온 세션이 나타납니다. 새 세션에 대해서는 **GPO 로드** 및 **프로파일 로드** 로그온 세그먼트가 나타납니다. 이러한 로그온 세그먼트가 새 세션에 대해 나타나지 않으면 RDS 호스트를 다시 시작해야 합니다.

Horizon Help Desk Tool 에 대한 세션 프로세스

세션 프로세스는 **세션** 탭에서 **컴퓨터 이름** 옵션에 있는 사용자 이름을 클릭하면 **프로세스** 탭에 나타납니다.

프로세스

각 세션에 대해 CPU 및 메모리 관련 프로세스에 대한 추가 세부 정보를 볼 수 있습니다. 예를 들어 세션에 대한 CPU 및 메모리 사용량이 비정상적으로 높다는 것을 알게 된 경우 **프로세스** 탭에서 프로세스에 대한 세부 정보를 볼 수 있습니다.

표 11-9. 세션 프로세스 세부 정보

옵션	설명
프로세스 이름	세션 프로세스의 이름입니다. 예: chrome.exe.
CPU	프로세스의 CPU 사용량(백분율)입니다.
메모리	프로세스의 메모리 사용량(KB)입니다.
디스크	메모리 디스크 IOPS입니다. 다음 수식을 사용하여 계산됩니다. (현재 시간의 총 I/O 바이트) - (현재 시간 1초 전의 총 I/O 바이트) 작업 관리자가 양수 값을 표시하는 경우 이 계산은 초당 0KB의 값을 표시할 수 있습니다.
사용자 이름	프로세스를 소유하는 사용자의 사용자 이름입니다.
호스트 CPU	세션이 할당된 가상 시스템의 CPU 사용량입니다.
호스트 메모리	세션이 할당된 가상 시스템의 메모리 사용량입니다.
프로세스	가상 시스템의 프로세스의 수입입니다.
새로 고침	새로 고침 아이콘은 프로세스의 목록을 새로 고칩니다.
프로세스 종료	실행 중인 프로세스를 종료합니다. 참고 프로세스를 종료하려면 헬프 데스크 관리자 역할이 있어야 합니다. 프로세스를 종료하려면 프로세스를 선택하고 프로세스 종료 버튼을 클릭합니다.

Horizon Help Desk Tool에 대한 애플리케이션 상태

세션 탭에서 **컴퓨터 이름** 옵션에 있는 사용자 이름을 클릭하면 **애플리케이션** 탭에서 애플리케이션의 상태 및 세부 정보를 볼 수 있습니다.

애플리케이션

각 애플리케이션에 대해 현재 상태 및 기타 세부 정보를 볼 수 있습니다.

표 11-10. 애플리케이션 세부 정보

옵션	설명
애플리케이션	애플리케이션의 이름입니다.
설명	애플리케이션에 대한 설명입니다.
상태	애플리케이션의 상태입니다. 애플리케이션이 실행되고 있는지 여부를 표시합니다.
호스트 CPU	세션이 할당된 가상 시스템의 CPU 사용량입니다.
호스트 메모리	세션이 할당된 가상 시스템의 메모리 사용량입니다.
애플리케이션	실행 중인 애플리케이션 목록입니다.
새로 고침	새로 고침 아이콘은 애플리케이션 목록을 새로 고칩니다.

Horizon Help Desk Tool 에서 데스크톱 또는 애플리케이션 세션 문제 해결

Horizon Help Desk Tool에서 사용자의 연결 상태를 기준으로 데스크톱 또는 애플리케이션 세션 문제를 해결할 수 있습니다.

사전 요구 사항

- Horizon Help Desk Tool를 시작합니다.

절차

- 1 사용자 카드에서 **세션** 탭을 클릭합니다.

CPU 및 메모리 사용량을 표시하고 Horizon Client, 가상 또는 게시된 데스크톱에 대한 정보를 포함하는 성능 카드가 표시됩니다.

2 문제 해결 옵션을 선택합니다.

옵션	조치
메시지 보내기	<p>게시된 데스크톱 또는 가상 데스크톱의 사용자에게 메시지를 전송합니다. [주의], [정보] 또는 [오류]를 포함하도록 메시지 심각도를 선택할 수 있습니다.</p> <p>메시지 보내기를 클릭하고 심각도 유형 및 메시지 세부 정보를 입력한 후 제출을 클릭합니다.</p>
원격 지원	<p>연결된 데스크톱 또는 애플리케이션 세션에 대한 원격 지원 티켓을 생성할 수 있습니다. 관리자는 원격 지원 티켓을 사용하여 사용자의 데스크톱을 제어하고 문제를 해결할 수 있습니다.</p> <p>원격 지원을 클릭하고 헬프 데스크 티켓 파일을 다운로드합니다. 티켓을 열고 원격 데스크톱의 사용자가 티켓을 수락할 때까지 기다립니다. Windows 데스크톱에서만 티켓을 열 수 있습니다. 사용자가 티켓을 수락한 후에는 해당 사용자와 채팅하고 사용자의 데스크톱 제어를 요청할 수 있습니다.</p> <p>참고 헬프 데스크 원격 지원 기능은 Microsoft 원격 지원을 기반으로 합니다. Microsoft 원격 지원을 설치하고 게시된 데스크톱에서 원격 지원 기능을 사용하도록 설정해야 합니다. Microsoft 원격 지원에 연결 또는 업그레이드 문제가 있는 경우 헬프 데스크 원격 지원이 시작되지 않을 수 있습니다. 자세한 내용은 Microsoft 웹 사이트에서 Microsoft 원격 지원 설명서를 참조하십시오.</p>
다시 시작	<p>가상 데스크톱에서 Windows 다시 시작 프로세스를 시작합니다. 이 기능은 게시된 데스크톱 또는 애플리케이션 세션에는 사용할 수 없습니다.</p> <p>VDI 다시 시작을 클릭합니다.</p>
연결 끊기	<p>데스크톱 또는 애플리케이션 세션을 연결 해제합니다.</p> <p>자세히 > 연결 끊기를 클릭합니다.</p>
로그오프	<p>게시된 데스크톱 또는 가상 데스크톱에 대한 로그오프 프로세스나 애플리케이션 세션에 대한 로그오프 프로세스를 시작합니다.</p> <p>자세히 > 로그오프를 클릭합니다.</p>
재설정	<p>가상 시스템의 재설정을 시작합니다. 이 기능은 게시된 데스크톱 또는 애플리케이션 세션에는 사용할 수 없습니다.</p> <p>자세히 > VM 재설정을 클릭합니다.</p> <p>참고 저장되지 않은 작업은 손실될 수 있습니다.</p>

VMware Logon Monitor 사용

VMware Logon Monitor는 Windows 사용자 로그인을 모니터링하고, 관리자, 지원 담당자 및 개발자가 느린 로그인 성능 문제를 해결하는 데 도움이 되도록 성능 메트릭을 보고합니다.

메트릭에는 로그인 시간, 로그인 스크립트 시간, CPU/메모리 사용량 및 네트워크 연결 속도가 포함됩니다. 또한 Logon Monitor는 로그인 프로세스에 대해 더 많은 정보를 제공하기 위해 다른 VMware 제품에서 메트릭을 받을 수도 있습니다.

지원되는 플랫폼

Logon Monitor는 Horizon Agent와 동일한 Windows 플랫폼을 지원합니다.

주요 기능

Logon Monitor는 다음과 같은 기능을 제공합니다.

- Horizon Agent의 일부분으로 설치됩니다. 이 서비스를 시작하려면 [KB 57051](#)을 참조하십시오.
- Horizon Help Desk Tool 타이밍 프로파일러와 통합됩니다. 로그인 관련 메트릭은 집계된 후 Horizon Agent 이벤트 데이터베이스로 전송됩니다.
- 고객이 쉽게 액세스할 수 있도록 로그를 파일 서버에 업로드할 수 있습니다.
- Logon Monitor에 로그인 관련 이벤트를 전송하는 Horizon Persona Management, App Volumes, UEM 및 Horizon Agent와 같은 기타 VMware 제품과 통합됩니다. Logon Monitor는 이러한 이벤트가 발생할 때 이벤트를 기록하여 로그인 흐름의 이벤트 및 이벤트가 지속되는 시간을 표시합니다.
- 동일한 시스템의 동시 로그온을 모니터링합니다.

로그

Logon Monitor는 서비스 상태 메시지 및 사용자 세션에 대한 로그 파일을 작성합니다. 기본적으로 모든 로그 파일은 C:\ProgramData\VMware\VMware Logon Monitor\Logs에 작성됩니다.

- 기본 로그: 기본 로그 파일인 vmlm.txt에는 로그온을 모니터링하기 전후에 발생하는 vmlm 서비스 및 세션 이벤트에 대한 모든 상태 메시지가 포함되어 있습니다. 이 로그를 확인하여 Logon Monitor가 올바르게 실행되고 있는지 확인합니다.
- 세션 로그: 세션 로그에는 사용자 로그인 세션과 관련된 모든 이벤트가 포함되어 있습니다. 이벤트는 로그온이 시작되고 단일 사용자 세션에 적용될 때만 이 로그에서 시작됩니다. 로그 끝에 작성된 요약은 가장 중요한 메트릭의 개요를 제공합니다. 느린 로그인 문제를 해결하려면 이 로그를 확인합니다. 로그온이 완료되면 추가 이벤트가 세션 로그에 작성되지 않습니다.

Logon Monitor 메트릭

Logon Monitor는 로그인, 그룹 정책, 사용자 프로파일 및 성능과 관련된 메트릭을 계산합니다. 이러한 메트릭은 로그인 시간 동안 관리자에게 최종 사용자 시스템에 대한 상세 보기를 제공하여 성능 병목 현상의 근본 원인을 파악하는 데 도움을 줍니다.

표 11-11. Logon Monitor 메트릭

메트릭	매개 변수	설명
로그온 시간	<ul style="list-style-type: none"> ■ 시작 ■ 종료 ■ 총 시간 	메트릭에는 게스트에서 로그온이 시작된 시간, 로그온이 완료되고 프로파일이 로드된 시간, 바탕 화면이 표시되는 시간, 게스트에서 로그온을 처리하는 데 소요된 총 시간이 포함됩니다. 게스트 외부에서 소요된 시간은 제외합니다.
세션 시작부터 로그온 시작까지 시간	총 시간	Windows에서 사용자 세션을 생성한 시간부터 로그온이 시작된 때까지의 시간입니다.
프로파일 동기화 시간	총 시간	Windows가 로그온 동안 사용자 프로파일을 조정하는 데 소요된 시간입니다.
셸 로드	<ul style="list-style-type: none"> ■ 시작 ■ 종료 ■ 총 시간 	Windows는 사용자 셸 로드의 시작 시간을 제공합니다. 종료 시간은 탐색기 창이 생성된 때입니다.
로그온에서 Hive 로드까지 시간	총 시간	메트릭은 로그온이 시작될 때부터 사용자 레지스트리 하이버가 로드될 때까지의 총 시간을 제공합니다.
Windows 폴더 리디렉션	<ul style="list-style-type: none"> ■ 시작 ■ 종료 ■ 총 시간 	Windows 폴더 리디렉션이 시작되고 완전히 적용되는 시간 및 Windows 폴더 리디렉션을 사용하도록 설정하는 총 시간과 관련된 메트릭입니다. 이 시간은 폴더 리디렉션이 처음 적용되었을 때 또는 새 파일이 리디렉션된 공유에 업로드되는 경우에 오래 걸릴 수 있습니다.
그룹 정책 시간	<ul style="list-style-type: none"> ■ 사용자 그룹 정책 적용 시간 ■ 시스템 그룹 정책 적용 시간 	게스트에 그룹 정책을 적용하는 것과 관련된 메트릭에는 사용자 그룹 정책 및 시스템 그룹 정책을 적용하는 데 걸린 시간이 포함됩니다.
프로파일 메트릭	<ul style="list-style-type: none"> ■ 프로파일 유형: 로컬, 로밍, 임시 ■ 프로파일 크기: 파일 수, 폴더 수, 총 메가바이트 	사용자 프로파일과 관련된 메트릭은 사용자 프로파일의 유형, 사용자 프로파일이 로컬 시스템에 저장되는지, 중앙 프로파일 저장소에 저장되는지 또는 로그 오프 후에 삭제되는지를 나타냅니다. 프로파일 크기에는 사용자 프로파일의 파일 수, 폴더의 총 수 및 총 크기(MB)에 대한 메트릭이 포함됩니다.
프로파일 크기 분포	<ul style="list-style-type: none"> ■ 0에서 1MB 사이의 파일 수 ■ 1MB에서 10MB 사이의 파일 수 ■ 10MB에서 100MB 사이의 파일 수 ■ 100MB에서 1GB 사이의 파일 수 ■ 1GB에서 10GB 사이의 파일 수 	사용자 프로파일에서 다양한 크기 범위에 해당하는 파일의 수입니다.

표 11-11. Logon Monitor 메트릭 (계속)

메트릭	매개 변수	설명
로그온 시 시작된 프로세스	<ul style="list-style-type: none"> 이름 프로세스 ID 상위 프로세스 ID 세션 ID 	이러한 값은 세션이 시작될 때 시작되고 로그온이 완료될 때까지 진행되는 각 프로세스에 대해 기록됩니다.
그룹 정책 로그온 스크립트 시간	총 시간	그룹 정책 로그온 스크립트 실행과 관련된 메트릭은 그룹 정책 로그온 스크립트 실행에 소요된 총 시간을 보고합니다.
그룹 정책 PowerShell 스크립트 시간	총 시간	그룹 정책 PowerShell 스크립트 실행과 관련된 메트릭은 그룹 정책 PowerShell 스크립트를 실행하는 데 소요된 시간을 나타냅니다.
메모리 사용량	<ul style="list-style-type: none"> 사용 가능한 바이트: 최소, 최대, 평균 커밋된 바이트: 최소, 최대, 평균 페이징된 풀: 최소, 최대, 평균 	로그온 동안 메모리 사용량과 관련된 WMI 메트릭입니다. 샘플링은 로그온이 완료될 때까지 수행됩니다. 기본적으로 사용하지 않도록 설정됩니다.
CPU 사용량	<ul style="list-style-type: none"> 유틸 CPU: 최소, 최대, 평균 사용자 CPU: 최소, 최대, 평균 커널 CPU: 최소, 최대, 평균 	로그온 시 CPU 사용량과 관련된 WMI 메트릭입니다. 샘플링은 로그온이 완료될 때까지 수행됩니다. 기본적으로 사용하지 않도록 설정됩니다.
로그온 스크립트는 동기 상태입니까?		그룹 정책 로그온 스크립트가 로그온과 동기식으로 실행되는지 또는 비동기식으로 실행되는지를 보고합니다.
네트워크 연결 상태	<ul style="list-style-type: none"> 손실됨 복원됨 	네트워크 연결이 활성 상태인지 또는 끊어졌는지를 보고합니다.
그룹 정책 소프트웨어 설치	<ul style="list-style-type: none"> 비동기: True/False 오류 코드 총 시간 	그룹 정책 소프트웨어 설치와 관련된 메트릭은 설치가 로그온과 동기 상태인지 또는 비동기 상태인지, 설치가 성공했는지 또는 실패했는지, 그룹 정책을 사용하여 소프트웨어를 설치하는 데 소요된 총 시간을 나타냅니다.
프로파일 볼륨에 대한 디스크 사용량	<ul style="list-style-type: none"> 사용자가 사용할 수 있는 디스크 공간 사용 가능한 디스크 공간 총 디스크 공간 	사용자 프로파일이 저장된 볼륨의 디스크 사용량과 관련된 메트릭입니다.
도메인 컨트롤러 검색	<ul style="list-style-type: none"> 오류 코드 총 시간 	도메인 컨트롤러 관련 메트릭입니다. 오류 코드는 도메인 컨트롤러에 연결하는 데 실패했는지 여부를 나타냅니다.
예상 네트워크 대역폭	대역폭	이벤트 ID 5327에서 수집된 값입니다.
네트워크 연결 세부 정보	<ul style="list-style-type: none"> 대역폭 느린 링크 임계값 느린 링크가 감지됨: True/False 	이벤트 ID 5314에서 수집된 값입니다.

표 11-11. Logon Monitor 메트릭 (계속)

메트릭	매개 변수	설명
로그온 시간에 영향을 줄 수 있는 설정	<ul style="list-style-type: none"> ■ 컴퓨터\관리 템플릿\로그온\컴퓨터 시작 및 로그인 시 항상 네트워크 대기 ■ 컴퓨터\관리 템플릿\로그온\사용자 로그인 시 다음 프로그램 실행 ■ 컴퓨터\관리 템플릿\사용자 프로파일\로밍 사용자 프로파일 대기 ■ 컴퓨터\관리 템플릿\사용자 프로파일\사용자에게 로밍 프로파일 또는 원격 홈 디렉토리가 있는 경우 네트워크에 대한 최대 대기 시간 설정 ■ 컴퓨터\관리 템플릿\그룹 정책\로그온 스크립트 지연 구성 ■ 사용자\관리 템플릿\시스템\로그온\사용자 로그인 시 다음 프로그램 실행 ■ 사용자\관리 템플릿\시스템\사용자 프로파일\로그온 시 동기화할 네트워크 디렉토리 지정, 로그오프 시간만 해당 	
Horizon Agent, Persona Management, App Volumes의 메트릭		Logon Monitor와 상호 작용하는 VMware 제품은 Logon Monitor 로그에 사용자 지정 메트릭을 보고합니다. 이러한 메트릭은 이러한 제품 중 하나가 로그인 시간에 부정적인 영향을 미칠 수 있는지를 확인하는 데 도움이 될 수 있습니다.

Logon Monitor 구성 설정

Windows 레지스트리 값을 사용하여 Logon Monitor 설정을 구성할 수 있습니다.

레지스트리 설정

구성 설정을 변경하려면 레지스트리 키 HKLM\Software\VMware, Inc.\VMware Logon Monitor로 이동합니다.

표 11-12. Logon Monitor 구성 값

레지스트리 키	유형	설명
RemoteLogPath	REG_SZ	로그를 업로드할 원격 공유 경로. 로그가 원격 로그 공유로 복사되면 RemoteLogPath 레지스트리 키로 지정된 폴더에 배치됩니다. 예: \\WserverWshareW%username%.%userdomain%. Logon Monitor는 필요에 따라 폴더를 생성합니다. 기본적으로 사용하지 않도록 설정됩니다. <ul style="list-style-type: none"> 원격 로그 폴더에 대한 UNC 경로 선택 사항으로 구성되지 않으면 로그가 업로드되지 않습니다. 선택 사항으로 로컬 환경 변수가 지원됩니다.
플래그	REG_DWORD	이 값은 Logon Monitor의 동작에 영향을 미치는 비트 마스크입니다. <ul style="list-style-type: none"> CPU 및 메모리 메트릭을 사용하거나 사용하지 않도록 설정하기 위해 설정 또는 제거할 값은 0x4입니다. 기본적으로 사용하지 않도록 설정됩니다. 프로세스 이벤트 및 로그인 스크립트 메트릭을 사용하도록 설정하기 위해 설정 또는 제거할 값은 0x8입니다. 기본적으로 사용하지 않도록 설정됩니다. Horizon 7과의 통합을 사용하거나 사용하지 않도록 설정할 값은 0x2입니다. 기본적으로 사용하도록 설정됩니다. 크래시 덤프가 사용되지 않도록 하기 위해 설정할 값은 0x1입니다. 덤프는 C:\ProgramData\VMware\VMware Logon Monitor\Data에 기록됩니다. 기본적으로 사용하지 않도록 설정됩니다. 원격 경로에서 사용자별 폴더를 생성하기 위해 설정된 값은 0x10입니다. 기본적으로 사용하지 않도록 설정됩니다.
LogMaxSizeMB	REG_DWORD	기본 로그의 최대 크기(MB)입니다. 기본값은 100MB입니다.
LogKeepDays	REG_DWORD	물리하기 전에 기본 로그를 보관할 최대 일 수입니다. 기본값은 7일입니다.

타이밍 프로파일러 설정

Logon Monitor는 Horizon 헬프 데스크 타이밍 프로파일러와 통합됩니다. 타이밍 프로파일러는 기본적으로 꺼져 있습니다.

- Logon Monitor에서 타이밍 프로파일러를 사용하여 이벤트 데이터베이스에 이벤트를 쓸 수 있게 하려면 `vdmadmin -l -timingProfiler -enable`을 실행합니다.
- Logon Monitor에서 타이밍 프로파일러를 사용하지 않도록 하려면 `vdmadmin -l -timingProfiler -disable`을 실행합니다.

VMware Horizon 성능 추적기 사용

VMware Horizon 성능 추적기는 원격 데스크톱에서 실행되고 디스플레이 프로토콜의 성능과 시스템 리소스 사용량을 모니터링하는 유틸리티입니다. 또한 애플리케이션 풀을 생성하고 Horizon 성능 추적기를 게시된 애플리케이션으로 실행할 수 있습니다.

VMware Horizon 성능 추적기 구성

원격 데스크톱에서 Horizon 성능 추적기를 실행할 수 있습니다. Horizon 성능 추적기를 게시된 애플리케이션으로 실행할 수도 있습니다.

Horizon 성능 추적기 기능

Horizon 성능 추적기는 다음 기능에 대한 중요한 데이터를 표시합니다.

표 11-13. Horizon 성능 추적기 기능

성능 모니터링	세부 정보
프로토콜 특정 데이터	<ul style="list-style-type: none"> 인코더 이름: 디스플레이 프로토콜에 사용된 인코더의 이름 사용된 대역폭: 샘플링 기간 동안의 디스플레이 프로토콜, PCoIP 또는 Blast에 대한 수신 및 송신 대역폭을 포함한 전체 대역폭 평균 초당 프레임 속도: 1초의 샘플링 기간 동안 인코딩된 이미징 프레임 수 오디오 켜짐: 오디오 기능이 켜져 있는지 여부 오디오 시작: 오디오 기능이 시작되었는지 여부 CPU 사용: <ul style="list-style-type: none"> 인코더 CPU: 현재 사용자 세션에서 디스플레이 프로토콜 인코더의 CPU 사용량 시스템 CPU: 시스템의 총 CPU 사용량
전송 유형	<ul style="list-style-type: none"> 클라이언트-원격 세션: 클라이언트-원격 피어에 사용되는 UDP 또는 TCP 프로토콜 전송 패키지 원격 세션-클라이언트: 원격 피어-클라이언트에 사용되는 UDP 또는 TCP 프로토콜 전송 패키지 Horizon Connection Server: 연결 서버 인스턴스에 연결하는 데 사용되는 UDP 또는 TCP 프로토콜 전송 패키지
시스템 상태	<ul style="list-style-type: none"> 예상 대역폭: Horizon Client와 Horizon Agent 간에 사용 가능한 전체 예상 대역폭 왕복: Horizon Agent와 Horizon Client 간의 왕복 지연 시간(밀리초)
세션 컨텍스트	<ul style="list-style-type: none"> DNS 이름, 도메인 이름, 터널링 여부, URL, 원격 IP 주소와 같은 서버 세부 정보 표시 번호, IP 주소, 키보드 및 마우스 레이아웃, 언어, 표준 시간대와 같은 클라이언트 시스템 세부 정보
실시간 프로토콜 전환	

참고 Horizon 성능 추적기는 Horizon Agent가 가상 데스크톱 세션에서 실행 중인 경우에만 데이터를 수집하고 표시합니다.

Horizon 성능 추적기에 대한 시스템 요구 사항

Horizon 성능 추적기는 다음 구성을 지원합니다.

표 11-14. Horizon 성능 추적기 시스템 요구 사항

시스템	요구 사항
가상 데스크톱 운영 체제	Horizon Agent를 지원하는 모든 운영 체제(Linux 에이전트 제외)
클라이언트 시스템 운영 체제	게시된 애플리케이션은 지원되지 않으므로 Linux용 Horizon Client 및 Windows 10 UWP용 Horizon Client를 제외한 모든 Horizon Client 버전이 지원됩니다.
디스플레이 프로토콜	VMware Blast 및 PCoIP

Horizon 성능 추적기 설치

Horizon 성능 추적기는 Horizon Agent 설치 관리자의 사용자 지정 설치 옵션입니다. 이 옵션은 기본적으로 선택되어 있지 않으므로 선택해야 합니다. Horizon 성능 추적기는 IPv4 및 IPv6 둘 다에 사용할 수 있습니다.

가상 데스크톱 또는 RDS 호스트에서 Horizon 성능 추적기를 설치할 수 있습니다. RDS 호스트에 설치하는 경우 게시된 애플리케이션으로 게시한 후 Horizon Client에서 게시된 애플리케이션을 실행할 수 있습니다. Horizon 7에서 게시된 데스크톱 및 애플리케이션 설정 문서를 참조하십시오.

설치하면 바탕 화면에 바로 가기가 생성됩니다.

Horizon 성능 추적기 그룹 정책 설정 구성

기본 설정을 변경하도록 그룹 정책 설정을 구성할 수 있습니다. [Horizon 성능 추적기 그룹 정책 설정 구성](#)의 내용을 참조하십시오.

Horizon 성능 추적기 그룹 정책 설정 구성

Horizon 성능 추적기를 구성하려면 에이전트 시스템에 Horizon 성능 추적기 ADMX 템플릿 파일(perf_tracker.admx)을 설치하고 로컬 그룹 정책 편집기를 사용하여 정책 설정을 구성합니다.

Horizon 7에 대한 그룹 정책 설정을 제공하는 모든 ADMX 파일은 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip에 있습니다. 여기서 x.x.x는 버전이고 yyyyyyy는 빌드 번호입니다.

<https://my.vmware.com/web/vmware/downloads>의 VMware 다운로드 사이트에서 파일을 다운로드할 수 있습니다. Desktop & End-User Computing에서 ZIP 파일이 포함되어 있는 VMware Horizon 7 다운로드를 선택합니다.

절차

- 1 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 파일에서 perf_tracker.admx 파일을 추출하고 에이전트 시스템의 %systemroot%\WPolicyDefinitions 폴더에 복사합니다.
- 2 VMware-Horizon-Extras-Bundle-x.x.x-yyyyyyy.zip 파일에서 perf_tracker.adml 파일을 추출하고 에이전트 시스템의 %systemroot%\WPolicyDefinitions\ 폴더에 있는 해당 언어 하위 폴더에 복사합니다.

예를 들어 en_us 버전의 perf_tracker.adml 파일을 %systemroot%\WPolicyDefinitions\en_us 하위 폴더에 복사합니다.

- 3 로컬 그룹 정책 편집기(gpedit.msc)를 시작하고 **컴퓨터 구성 > 관리 템플릿 > VMware Horizon 성능 추적기**로 이동합니다.

4 그룹 정책 설정을 편집합니다.

설정	설명
Horizon 성능 추적기 기본 설정	사용하도록 설정한 경우 Horizon 성능 추적기가 데이터를 수집하는 빈도(초)를 설정할 수 있습니다.
원격 데스크톱 연결에서 Horizon 성능 추적기 자동 시작을 사용하도록 설정합니다.	사용하도록 설정한 경우 사용자가 원격 데스크톱 연결에 로그인하면 Horizon 성능 추적기가 자동으로 시작됩니다. 이 기본 설정 GPO 설정을 지우려면 사용 안 함 을 선택합니다.
원격 애플리케이션 연결에서 Horizon 성능 추적기 자동 시작 사용	사용하도록 설정한 경우 사용자가 원격 애플리케이션 연결에 로그인하면 Horizon 성능 추적기가 자동으로 시작됩니다. 이 기본 설정 GPO 설정을 지우려면 사용 안 함 을 선택합니다.

5 변경 사항을 적용하려면 에이전트 시스템에서 Horizon 성능 추적기를 다시 시작합니다.

Horizon 성능 추적기 실행

Horizon Client를 사용하여 Horizon 성능 추적기를 원격 데스크톱 내부에서 또는 게시된 애플리케이션으로 실행할 수 있습니다.

사용 중인 Horizon Client 플랫폼이 여러 세션을 지원하는 경우 다양한 팜에서 여러 Horizon 성능 추적기 게시된 애플리케이션을 실행할 수 있습니다. 다중 세션을 지원하는 Windows 및 Mac 클라이언트에서 개요 창의 시스템 이름은 게시된 애플리케이션이 시작된 원본 팜을 식별합니다. Android 및 iOS 클라이언트 및 HTML Access에서는 한 번에 하나의 열린 세션만 지원됩니다. 다른 팜에서 두 번째 세션을 여는 경우 첫 번째 세션이 닫힙니다.

사전 요구 사항

- Horizon 성능 추적기를 설치 및 구성합니다. [VMware Horizon 성능 추적기 구성](#)의 내용을 참조하십시오.
- Horizon 성능 추적기 그룹 정책 설정을 구성합니다. [Horizon 성능 추적기 그룹 정책 설정 구성](#)의 내용을 참조하십시오.

절차

- 원격 데스크톱에서 Horizon 성능 추적기를 실행하려면 Horizon Client 또는 HTML Access를 사용하여 서버에 연결하고 원격 데스크톱을 시작합니다.

원격 데스크톱을 열 때 Horizon 성능 추적기가 자동으로 시작되지 않으면 Windows 데스크톱에서 **VMware Horizon 성능 추적기** 바로 가기를 두 번 클릭하거나 Windows 애플리케이션을 시작할 때와 같은 방식으로 Horizon 성능 추적기를 시작할 수 있습니다.

개요 창이나 부동 표시줄을 표시하고 애플리케이션을 종료하는 옵션을 선택하려면 원격 데스크톱의 시스템 트레이에서 VMware Horizon 성능 추적기 아이콘을 마우스 오른쪽 버튼으로 클릭합니다.

- Horizon 성능 추적기를 게시된 애플리케이션으로 실행하려면 Horizon Client 또는 HTML Access를 사용하여 서버에 연결하고 Horizon 성능 추적기 게시된 애플리케이션을 시작합니다.

Horizon 성능 추적기 게시된 애플리케이션을 사용하는 방법은 사용 중인 클라이언트 유형에 따라 다릅니다. Linux용 Horizon Client 또는 Windows 10 UWP용 Horizon Client를 사용하여 Horizon 성능 추적기를 게시된 애플리케이션으로 실행할 수는 없습니다.

- Windows용 Horizon Client를 사용하는 경우 VMware Horizon 성능 추적기 아이콘이 Windows 클라이언트 시스템의 시스템 트레이에 표시됩니다. 이 아이콘을 두 번 클릭하여 Windows 클라이언트에서 Horizon 성능 추적기를 열 수 있습니다. 이 아이콘을 마우스 오른쪽 버튼으로 클릭하여 개요 창 또는 부동 표시줄을 표시하고 애플리케이션을 종료하는 옵션을 선택할 수 있습니다.
- Mac용 Horizon Client를 사용하는 경우 VMware Horizon 성능 추적기 아이콘이 Mac 클라이언트 시스템의 메뉴 표시줄에 표시됩니다. 이 아이콘을 두 번 클릭하여 Mac 클라이언트에서 Horizon 성능 추적기를 열 수 있습니다. 이 아이콘을 마우스 오른쪽 버튼으로 클릭하여 개요 창 또는 부동 표시줄을 표시하고 애플리케이션을 종료하는 옵션을 선택할 수도 있습니다.
- Android용 Horizon Client 또는 iOS용 Horizon Client를 사용할 경우 VMware Horizon 성능 추적기 아이콘이 Horizon Client의 Unity Touch 사이드바에 표시됩니다. 이 아이콘을 길게 터치하여 개요 창 및 부동 표시줄을 표시하고 애플리케이션을 종료하는 옵션을 선택할 수 있습니다.
- HTML Access를 사용할 경우 VMware Horizon 성능 추적기 아이콘이 HTML Access 사이드바에 표시됩니다. 이 아이콘을 마우스 오른쪽 버튼으로 클릭하여 개요 창 또는 부동 표시줄을 표시하고 애플리케이션을 종료하는 옵션을 선택할 수 있습니다.

다음에 수행할 작업

Horizon 성능 추적기에 표시되는 데이터에 대한 자세한 내용은 [VMware Horizon 성능 추적기 구성](#)을 참조하십시오.

시스템 상태 모니터링

Horizon Administrator에서 시스템 상태 대시보드를 사용하면 Horizon 7 작업 또는 최종 사용자 가 원격 데스크톱에 액세스하는 데 영향을 줄 수 있는 문제를 신속하게 파악할 수 있습니다.

Horizon Administrator 화면의 왼쪽 상단에 있는 시스템 상태 대시보드에는 Horizon 7 작업에 대한 보고서를 볼 수 있는 다양한 링크가 제공됩니다.

세션	원격 데스크톱 및 애플리케이션 세션의 상태 정보를 표시하는 세션 화면에 대한 링크를 제공합니다.
문제가 있는 vCenter VM	vCenter 가상 시스템, RDS 호스트 및 Horizon 7에서 문제가 있는 것으로 표시한 시스템 정보가 표시되는 시스템 화면에 대한 링크를 제공합니다.
문제가 있는 RDS 호스트	Horizon 7에서 문제가 있는 것으로 표시한 RDS 호스트 정보를 보여 주는 시스템 화면 내 RDS 호스트 탭에 대한 링크를 제공합니다.

이벤트	오류 이벤트 및 경고 이벤트에 대해 필터링된 이벤트 화면의 링크를 제공합니다.
시스템 상태	Horizon 7 구성 요소의 상태, 3.4 이상 버전에 대한 등록된 Unified Access Gateway 세부 정보, vSphere 구성 요소, 도메인, 데스크톱 및 데이터스토어 사용량에 대한 요약 정보를 보여 주는 [대시보드] 화면에 대한 링크를 제공합니다.

시스템 상태 대시보드는 각 항목에 대해 번호가 매겨진 링크를 표시합니다. 이 값은 연결된 보고서로 상세한 정보를 제공하는 항목 수를 나타냅니다.

Horizon 7의 이벤트 모니터링

이벤트 데이터베이스는 연결 서버 호스트 또는 그룹, Horizon Agent, Horizon Administrator에서 발생하는 이벤트 정보를 저장하고 대시보드를 통해 이벤트의 개수를 알려 줍니다. 이벤트 화면에서 이벤트를 자세히 검토할 수 있습니다.

참고 제한된 시간 동안에만 Horizon Administrator 인터페이스에 이벤트가 표시됩니다. 이 시점 이후에는 내역 데이터베이스 테이블에서만 이벤트를 볼 수 있습니다. Microsoft SQL Server 또는 Oracle 데이터베이스 보고 도구를 사용해 데이터베이스 테이블의 이벤트를 검토할 수 있습니다. 자세한 내용은 Horizon 7 통합 문서를 참조하십시오.

참고 이벤트 데이터베이스를 사용할 수 없게 된 경우 Horizon 7에서는 이러한 사용 불가능 기간 동안 발생하는 이벤트의 감사 추적을 유지하고, 사용할 수 있게 되면 이벤트 데이터베이스에 해당 이벤트를 저장합니다. Horizon Administrator 인터페이스에서 이러한 이벤트를 보려면 이벤트 데이터베이스와 연결 서버를 다시 시작해야 합니다.

Horizon Administrator에서는 이벤트를 모니터링할 수 있을 뿐만 아니라 분석 소프트웨어가 이벤트 데이터에 액세스할 수 있도록 Horizon 7 이벤트를 Syslog 형식으로 생성할 수도 있습니다. Horizon 7 설치 문서에서 **-i** 옵션을 사용하여 **Syslog 형식으로 Horizon 7 이벤트 로그 메시지 생성** 및 “Syslog 서버의 이벤트 로깅 구성”을 참조하십시오.

사전 요구 사항

Horizon 7 설치 문서에 따라 이벤트 데이터베이스를 생성 및 구성합니다.

절차

- 1 Horizon Administrator에서 **모니터링 > 이벤트**를 선택합니다.
- 2 (선택 사항) 이벤트 창에서 이벤트의 시간 범위를 선택하고 이벤트에 필터링을 적용하고 하나 이상의 열에 이벤트 목록을 정렬할 수 있습니다.

Horizon 7 이벤트 메시지

Horizon 7는 시스템 상태가 변경되거나 문제가 발생할 때마다 이벤트를 보고합니다. 이벤트 메시지의 정보를 사용하여 적절한 작업을 수행할 수 있습니다.

다음 표에는 Horizon 7이 보고하는 이벤트 유형이 나와 있습니다.

표 11-15. Horizon 7 가 보고하는 이벤트 유형

이벤트 유형	설명
감사 실패 또는 감사 성공	관리자나 사용자가 Horizon 7의 작업 또는 구성에 적용하는 변경 사항의 실패 또는 성공을 보고합니다.
오류	Horizon 7에서 실패한 작업을 보고합니다.
정보	Horizon 7 내의 정상 작업을 보고합니다.
경고	시간 경과에 따라 더 심각한 문제로 이어질 수 있는 작업 또는 구성 설정의 사소한 문제를 보고합니다.

감사 실패, 오류 또는 경고 이벤트와 연결된 메시지가 나타날 경우 약간의 작업을 수행해야 할 수도 있습니다. 감사 성공 또는 정보 이벤트를 위해서는 임의의 작업을 수행할 필요가 없습니다.

Horizon 7 의 진단 정보 수집

진단 정보를 수집해 VMware 기술 지원의 Horizon 7 문제 진단 및 해결 작업을 지원할 수 있습니다.

다양한 Horizon 7 구성 요소에 대한 진단 정보를 수집할 수 있습니다. Horizon 7 구성 요소에 따라 다양한 방법으로 정보를 수집할 수 있습니다.

- **Horizon Agent의 데이터 수집 도구 번들 생성**

vdmadmin 명령으로 DCT(데이터 수집 도구) 번들을 생성해 VMware 기술 지원의 Horizon Agent 문제 해결 작업을 지원할 수 있습니다. vdmadmin을 사용하지 않고 수동으로 DCT 번들을 얻을 수도 있습니다.

- **Windows용 Horizon Client에 대한 진단 정보 저장**

Windows용 Horizon Client 사용 중 문제가 발생하고 일반 네트워크 문제 해결 기술을 사용하여 문제를 해결할 수 없는 경우, 구성에 대한 로그 파일 복사본과 정보를 저장해 둘 수 있습니다.

- **지원 스크립트를 사용한 View Composer 진단 정보 수집**

View Composer 지원 스크립트를 사용해 구성 데이터를 수집하고 View Composer 로그 파일을 생성할 수 있습니다. 이 정보는 VMware 고객 지원이 View Composer에서 발생하는 모든 문제를 진단하는데 사용됩니다.

- **Horizon 연결 서버의 진단 정보 수집**

지원 도구를 사용해 로깅 수준을 설정하고 Horizon 연결 서버 로그 파일을 생성할 수 있습니다.

- **콘솔에서 Horizon Agent, Horizon Client 또는 Horizon 연결 서버에 대한 진단 정보 수집**

콘솔에 직접 액세스하는 경우 지원 스크립트를 사용하여 Horizon Agent를 실행하는 연결 서버, Horizon Client 또는 원격 데스크톱에 대한 로그 파일을 생성할 수 있습니다. 이 정보는 VMware 기술 지원이 이들 구성 요소에서 발생하는 모든 문제를 진단하는데 사용됩니다.

Horizon Agent 의 데이터 수집 도구 번들 생성

vdmadmin 명령으로 DCT(데이터 수집 도구) 번들을 생성해 VMware 기술 지원의 Horizon Agent 문제 해결 작업을 지원할 수 있습니다. vdmadmin을 사용하지 않고 수동으로 DCT 번들을 얻을 수도 있습니다.

편의를 위해 연결 서버 인스턴스에서 vdmadmin 명령을 사용하여 원격 데스크톱에서 DCT 번들을 요청할 수 있습니다. 번들이 연결 서버로 반환됩니다.

또는 특정 원격 데스크톱에 로그인한 다음 support 명령을 실행하여 해당 데스크톱에 DCT 번들을 생성할 수 있습니다. UAC(사용자 계정 컨트롤)가 켜져 있는 경우에는 이 방식으로 DCT 번들을 얻어야 합니다.

절차

- 1 필요한 권한이 있는 사용자로 로그인하십시오.

옵션	조치
View 연결 서버에서 vdmadmin 사용	연결 서버의 표준 인스턴스나 복제본 인스턴스에 관리자 역할을 가진 사용자로 로그인합니다.
원격 데스크톱	관리 권한을 가진 사용자로 원격 데스크톱에 로그인합니다.

- 2 명령 프롬프트를 열고 명령을 실행하여 DCT 번들을 생성하십시오.

옵션	조치
View 연결 서버에서 vdmadmin 사용	출력 번들 파일, 데스크톱 풀, 시스템의 이름을 지정하려면 -outfile, -d 및 -m 옵션을 vdmadmin 명령과 함께 사용하십시오. vdmadmin -A [-b authentication_arguments] -getDCT -outfile local_file -d desktop -m machine
원격 데스크톱	디렉토리를 c:\Program Files\VMware\VMware View\Agent\WDCT로 변경한 후 다음 명령을 실행합니다. support

특정 출력 파일에 번들을 작성하는 명령입니다.

예제:vdmadmin을 사용하여 Horizon Agent 의 번들 파일 생성

데스크톱 풀 dtpool2의 시스템 machine1에 대한 DCT 번들을 생성하고 압축 파일 C:\Wmyfile.zip에 작성하십시오.

```
vdmadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\Wmyfile.zip
```

다음에 수행할 작업

기존에 지원을 요청한 경우 DCT 번들 파일을 첨부해 지원 요청을 업데이트할 수 있습니다.

Windows용 Horizon Client 에 대한 진단 정보 저장

Windows용 Horizon Client 사용 중 문제가 발생하고 일반 네트워크 문제 해결 기술을 사용하여 문제를 해결할 수 없는 경우, 구성에 대한 로그 파일 복사본과 정보를 저장해 둘 수 있습니다.

진단 정보를 저장하고 VMware 기술 지원에 연락하기 전에 Windows용 Horizon Client의 연결 문제를 해결하기 위한 시도를 해 볼 수 있습니다. 자세한 내용은 Horizon 7에서 가상 데스크톱 설정 문서에서 "Horizon Client와 Horizon 연결 서버 간의 연결 문제"를 참조하십시오.

다른 Horizon Client 플랫폼에 대한 지원 데이터 수집 방법에 대한 자세한 내용은 해당 플랫폼의 설치 및 설정 가이드를 참조하십시오. 예를 들어 Mac용 Horizon Client의 경우 Mac용 VMware Horizon Client 설치 및 설정 가이드 항목을 참조하십시오.

절차

- 1 Horizon Client에서 **지원 정보**를 클릭하거나 원격 데스크톱 메뉴에서 **옵션 > 지원 정보**를 선택합니다.
- 2 **지원 정보** 창에서 **지원 데이터 수집**을 클릭하고 메시지가 나타나면 **예**를 클릭합니다.
명령 창에는 정보 수집 진행 상황이 표시됩니다. 이 작업은 몇 분 정도 걸릴 수 있습니다.
- 3 명령 창에서 Horizon Client의 구성을 테스트할 Horizon 연결 서버 인스턴스의 URL을 입력하고, 필요한 경우 Horizon 7 프로세스의 진단 덤프를 생성하도록 선택하여 프롬프트에 응답합니다.
정보는 클라이언트 시스템의 데스크톱에 있는 폴더의 zip 파일에 작성됩니다.
- 4 VMware 웹 사이트의 지원 페이지에서 지원 요청을 파일에 보존하고 출력 zip 파일을 첨부하십시오.

지원 스크립트를 사용한 View Composer 진단 정보 수집

View Composer 지원 스크립트를 사용해 구성 데이터를 수집하고 View Composer 로그 파일을 생성할 수 있습니다. 이 정보는 VMware 고객 지원이 View Composer에서 발생하는 모든 문제를 진단하는데 사용됩니다.

사전 요구 사항

View Composer가 설치된 컴퓨터에 로그인하십시오.

지원 스크립트를 실행하려면 Windows 스크립트 호스트 유틸리티(cscript)를 사용해야 하므로 cscript 사용 방법을 숙지하십시오. <http://technet.microsoft.com/library/bb490887.aspx>를 참조하십시오.

절차

- 1 명령 프롬프트 창을 열고 C:\Program Files\VMware\VMware View Composer 디렉토리로 변경하십시오.
기본 디렉토리에 소프트웨어를 설치하지 않은 경우 적절한 드라이브 문자 및 경로로 대체하십시오.
- 2 svi-support 스크립트를 실행하려면 명령을 입력하십시오.

```
cscript ".\svi-support.wsf" /zip
```

/? 옵션을 사용해 스크립트에서 사용할 수 있는 다른 명령 옵션 정보를 표시할 수 있습니다.

스크립트가 종료되면 출력 파일의 이름 및 위치를 알려줍니다.

- 3 VMware 웹 페이지의 지원 페이지에 지원 요청을 제출하고 출력 파일을 첨부하십시오.

Horizon 연결 서버의 진단 정보 수집

지원 도구를 사용해 로깅 수준을 설정하고 Horizon 연결 서버 로그 파일을 생성할 수 있습니다.

지원 도구는 연결 서버의 로깅 데이터를 수집합니다. 이 정보는 VMware 기술 지원이 연결 서버에서 발생하는 모든 문제를 진단하는 데 도움이 됩니다. 지원 도구는 Horizon Client나 Horizon Agent의 진단 정보를 수집하는 용도로 설계되지 않았습니다. 지원 스크립트를 대신 사용해야 합니다. [콘솔에서 Horizon Agent, Horizon Client 또는 Horizon 연결 서버에 대한 진단 정보 수집](#)을 참조하십시오.

사전 요구 사항

연결 서버의 표준 인스턴스나 복제본 인스턴스에 **관리자** 역할의 사용자로 로그인합니다.

절차

- 1 시작 > 모든 프로그램 > VMware > View 연결 서버 로그 레벨 설정을 선택합니다.
- 2 선택 텍스트 상자에 숫자 값을 입력해 로깅 수준을 설정하고 Enter 키를 누르십시오.

옵션	설명
0	기본 값으로 로깅 수준을 다시 설정합니다.
1	일반 로깅 수준을 선택합니다.
2	디버그 로깅 수준을 선택합니다(기본값).
3	전체 로깅을 선택합니다.

사용한 선택 수준에 따라 시스템에서 로그 정보를 기록하기 시작합니다.

- 3 연결 서버의 동작에 대해 충분한 정보를 수집했으면 시작 > 모든 프로그램 > VMware > View 연결 서버 로그 번들 생성을 선택합니다.

지원 도구에서 연결 서버 인스턴스의 데스크톱에 위치한 vdm-sdct 폴더에 로그 파일을 작성합니다.

- 4 VMware 웹 페이지의 지원 페이지에 지원 요청을 제출하고 출력 파일을 첨부하십시오.

콘솔에서 Horizon Agent , Horizon Client 또는 Horizon 연결 서버에 대한 진단 정보 수집

콘솔에 직접 액세스하는 경우 지원 스크립트를 사용하여 Horizon Agent를 실행하는 연결 서버, Horizon Client 또는 원격 데스크톱에 대한 로그 파일을 생성할 수 있습니다. 이 정보는 VMware 기술 지원이 이들 구성 요소에서 발생하는 모든 문제를 진단하는데 사용됩니다.

사전 요구 사항

정보를 수집하려는 시스템에 로그인하십시오. 관리자 권한을 가진 사용자로 로그인해야 합니다.

- Horizon Agent의 경우 Horizon Agent가 설치되어 있는 가상 시스템에 로그인하십시오.
- Horizon Client의 경우 Horizon Client가 설치되어 있는 시스템에 로그인하십시오.
- 연결 서버의 경우 연결 서버 호스트에 로그인하십시오.

절차

- 1 명령 프롬프트 창을 열고 진단 정보를 수집하려는 Horizon 7 구성 요소에 해당하는 디렉토리로 변경합니다.

옵션	설명
Horizon Agent	C:\Program Files\VMware View\Agent\WDCT 디렉토리로 변경하십시오.
Horizon Client	C:\Program Files\VMware View\Client\WDCT 디렉토리로 변경하십시오.
View 연결 서버	C:\Program Files\VMware View\Server\WDCT 디렉토리로 변경하십시오.

기본 디렉토리에 소프트웨어를 설치하지 않은 경우 적절한 드라이브 문자 및 경로로 대체하십시오.

- 2 지원 스크립트를 실행하려면 명령을 입력하십시오.

```
.\support.bat [loglevels]
```

고급 로깅을 사용하도록 설정하려면 loglevels 옵션을 지정하고 메시지가 나타날 때 로깅 수준에 대한 숫자 값을 입력하십시오.

옵션	설명
0	기본 값으로 로깅 수준을 다시 설정합니다.
1	일반 로깅 수준을 선택합니다.
2	디버그 로깅 수준을 선택합니다(기본값).
3	전체 로깅을 선택합니다.
4	PCoIP에 대해 정보 로깅을 선택합니다(Horizon Agent 및 Horizon Client에만 해당).
5	PCoIP에 대해 디버그 로깅을 선택합니다(Horizon Agent 및 Horizon Client에만 해당).
6	가상 채널에 대해 정보 로깅을 선택합니다(Horizon Agent 및 Horizon Client에만 해당).
7	가상 채널에 대해 디버그 로깅을 선택합니다(Horizon Agent 및 Horizon Client에만 해당).
8	가상 채널에 대해 추적 로깅을 선택합니다(Horizon Agent 및 Horizon Client에만 해당).

스크립트가 데스크톱의 vdm-sdct 폴더에 압축 로그 파일을 작성합니다.

- 3 View Composer 게스트 에이전트 로그는 C:\Program Files\Common Files\VMware\View Composer Guest Agent svi-ga-support 디렉토리에서 확인할 수 있습니다.
- 4 VMware 웹 페이지의 지원 페이지에 지원 요청을 제출하고 출력 파일을 첨부하십시오.

지원 요청 업데이트

지원 웹 사이트에서 기존 지원 요청을 업데이트할 수 있습니다.

지원 요청을 파일로 제출하고 나면 support 또는 svi-support 스크립트의 출력 파일을 요청하는 VMware 기술 지원의 e-메일 요청을 받을 수도 있습니다. 스크립트를 실행할 경우 출력 파일의 이름 및 위치를 알려줍니다. e-메일 메시지에 응답하고 응답에 출력 파일을 첨부합니다.

출력 파일이 너무 커서 첨부할 수 없는 경우(10MB 이상) VMware 기술 지원에 문의하여 지원 요청 번호를 알려주고 FTP 업로드 지침을 요청합니다. 또는 지원 웹 사이트에서 기존 지원 요청에 파일을 첨부할 수 있습니다.

절차

- 1 VMware 웹 사이트에 있는 지원 페이지를 방문하여 로그인하십시오.
- 2 **지원 요청 기록**을 클릭하고 적용 가능한 지원 요청 번호를 찾습니다.
- 3 지원 요청을 업데이트하고 support 또는 svi-support 스크립트를 실행하여 얻은 출력을 첨부하십시오.

보안 서버와 Horizon 연결 서버와의 연결 실패 문제 해결

연결 서버 인스턴스와의 연결에 실패할 경우 보안 서버가 작동하지 않을 수 있습니다.

문제

보안 서버가 연결 서버와의 연결에 실패할 경우 다음과 같은 보안 서버 문제가 발생할 수 있습니다.

- 보안 서버를 두 번째로 설치할 경우 보안 서버가 연결 서버에 연결할 수 없습니다.
- Horizon Client가 Horizon 7에 연결할 수 없습니다. 다음 오류 메시지가 표시됩니다. View 연결 서버 인증에 실패했습니다. 데스크톱에 보안 연결을 제공하는 게이트웨이를 사용할 수 없습니다. 네트워크 관리자에게 문의하십시오.
- 보안 서버가 Horizon Administrator 대시보드에 다운으로 표시됩니다.

원인

이 문제는 보안 서버 설치를 시작하고 보안 서버 연결 암호를 입력한 후 작업이 취소 또는 중단된 경우에 발생할 수 있습니다.

해결책

Horizon 7 환경에서 보안 서버를 유지하려면 다음 단계를 수행하십시오.

- 1 Horizon Administrator에서 **View 구성 > 서버**를 선택합니다.
- 2 **보안 서버** 탭에서 보안 서버를 선택하고 **추가 명령** 드롭다운 메뉴에서 **업그레이드 또는 다시 설치 준비**를 선택한 다음 **확인**을 클릭합니다.
- 3 **연결 서버** 탭에서 보안 서버와 연결할 연결 서버 인스턴스를 선택하고 **추가 명령** 드롭다운 메뉴에서 **보안 서버 연결 암호 지정**을 선택한 다음 암호를 입력하고 **확인**을 클릭합니다.
- 4 보안 서버를 다시 설치합니다.

Horizon 7 환경에서 보안 서버 항목을 제거하려면 `vdadmin -S` 명령을 실행하십시오.

예: `vdadmin -S -r -s security_server_name`

Horizon 7 Server 인증서 해지 검사 문제 해결

서버의 TLS 인증서에 대해 인증서 해지 검사를 수행할 수 없는 경우 보안 Horizon Client 연결에 사용되는 보안 서버 또는 연결 서버 인스턴스가 View Administrator에 빨간색으로 표시될 수 있습니다.

문제

Horizon Administrator 대시보드에서 보안 서버 또는 연결 서버 아이콘이 빨간색으로 표시됩니다. Horizon 7 서버 상태에는 서버의 인증서를 확인할 수 없습니다.라는 메시지가 표시됩니다.

원인

조직에서 프록시 서버를 사용해 인터넷에 액세스하거나 연결 서버 인스턴스가 방화벽 또는 기타 컨트롤 때문에 해지 검사를 제공하는 서버에 도달할 수 없는 경우 인증서 해지 검사가 실패할 수 있습니다.

연결 서버 인스턴스가 자체 인증서와 연결된 보안 서버의 인증서에 대한 인증서 해지 검사를 수행합니다. 기본적으로 VMware Horizon View 연결 서버 서비스는 LocalSystem 계정으로 시작됩니다. LocalSystem에서 실행할 경우 연결 서버 인스턴스가 Internet Explorer에 구성된 프록시 설정을 사용해 CRL DP URL 또는 OCSP 응답자에 액세스하여 인증서의 해지 상태를 확인할 수 없습니다.

Microsoft Netshell 명령을 사용해 프록시 설정을 연결 서버 인스턴스로 가져와 서버가 인터넷의 인증서 해지 검사 사이트에 액세스하도록 할 수 있습니다.

해결책

- 1 연결 서버 컴퓨터에서 **관리자 권한으로 실행** 설정으로 명령줄 창을 엽니다.

예를 들어, **시작**을 클릭하고 **cmd**를 입력한 다음 cmd.exe 아이콘을 마우스 오른쪽 단추로 클릭하고 **관리자 권한으로 실행**을 선택합니다.

- 2 **netsh**를 입력하고 Enter 키를 누릅니다.

- 3 **winhttp**를 입력하고 Enter 키를 누릅니다.

- 4 **show proxy**를 입력하고 Enter 키를 누릅니다.

Netshell이 프록시가 DIRECT 연결로 설정되었음을 표시합니다. 이 설정을 사용하면 조직에서 프록시를 사용할 경우 연결 서버 컴퓨터가 인터넷에 연결할 수 없습니다.

- 5 프록시 설정을 구성합니다.

예를 들어, netsh winhttp> 프롬프트에 **import proxy source=ie**를 입력합니다.

시스템에서 프록시 설정을 연결 서버 컴퓨터로 가져옵니다.

- 6 **show proxy**를 입력하여 프록시 설정을 확인합니다.

- 7 VMware Horizon View 연결 서버 서비스를 다시 시작합니다.

- 8 Horizon Administrator 대시보드에서 보안 서버 또는 연결 서버 아이콘이 녹색으로 표시되는지 확인합니다.

스마트 카드 인증서 해지 검사 문제 해결

사용자가 스마트 카드 인증서 해지 검사를 구성하지 않은 경우 스마트 카드가 연결된 연결 서버 인스턴스 또는 보안 서버가 서버의 TLS 인증서에 대한 인증서 해지 검사를 수행할 수 없습니다.

문제

조직에서 프록시 서버를 사용해 인터넷에 액세스하거나 연결 서버 인스턴스 또는 보안 서버가 방화벽 또는 기타 컨트롤 때문에 해지 검사를 제공하는 서버에 도달할 수 없는 경우 인증서 해지 검사가 실패할 수 있습니다.

중요 CRL 파일이 최신 버전인지 확인하십시오.

원인

Horizon 7에서는 인증서 해지 목록(CRL) 및 온라인 인증서 상태 프로토콜(OCSP)을 사용하여 인증서 해지 확인을 지원합니다. CRL은 인증서를 발행한 CA(인증 기관)에서 게시한 해지된 인증서 목록입니다. OCSP는 X.509 인증서의 해지 상태를 얻는 데 사용되는 인증서 유효성 검사 프로토콜입니다. CA는 연결 서버 인스턴스 또는 보안 서버 호스트에서 액세스할 수 있어야 합니다. 이 문제는 스마트 카드 인증서의 해지 검사를 구성한 경우에 발생할 수 있습니다. [스마트 카드 인증서 해지 검사 사용](#)의 내용을 참조하십시오.

해결책

- 1 Horizon 7 Server에서 경로로 사용할 CA 웹 사이트에서 최신 CRL을 다운로드하는 절차를 직접(수동으로) 생성합니다.
- 2 연결 서버 또는 보안 서버 호스트의 TLS/SSL 게이트웨이 구성 폴더에 `locked.properties` 파일을 생성 또는 편집합니다.
예: `install_directory\VMware\VMware View\Server\SSLgateway\conf\locked.properties`
- 3 `locked.properties` 파일의 `enableRevocationChecking` 및 `crlLocation` 속성을 CRL이 저장된 로컬 경로에 추가합니다.
- 4 변경 내용을 적용하려면 연결 서버 서비스 또는 보안 서버 서비스를 다시 시작합니다.

문제 해결 추가 정보

VMware 기술 자료 문서에서 문제 해결 정보를 추가로 확인할 수 있습니다.

VMware 제품의 새로운 문제 해결 정보를 VMware 기술 자료(KB)에 계속 업데이트하고 있습니다.

Horizon 7 문제 해결에 대한 자세한 내용은 VMware KB 웹 사이트의 KB 문서를 참조하십시오.

<http://kb.vmware.com/selfservice/microsites/microsite.do>

vdmadmin 명령 사용

vdmadmin 명령줄 인터페이스를 사용해 연결 서버 인스턴스에서 다양한 관리 작업을 수행할 수 있습니다.

vdmadmin을 사용해 Horizon Administrator 사용자 인터페이스에서 실행할 수 없는 관리 작업을 수행하거나 스크립트에서 자동으로 실행해야 하는 관리 작업을 수행할 수 있습니다.

Horizon Administrator, Horizon 7 cmdlet 및 vdmadmin에서 실행할 수 있는 작업을 비교하려면 Horizon 7 통합 문서를 참조하십시오.

- **vdmadmin 명령 사용**

vdmadmin 명령 구문은 해당 작업을 제어합니다.

- **-A 옵션을 사용하여 Horizon Agent 로그인 구성**

vdmadmin 명령을 -A 옵션과 함께 사용해 Horizon Agent에서 로깅을 구성할 수 있습니다.

- **-A 옵션을 사용하여 IP 주소 재정의**

vdmadmin 명령을 -A 옵션과 함께 사용하여 Horizon Agent에서 보고한 IP 주소를 재정의할 수 있습니다.

- **-F 옵션을 사용하여 외부 보안 주체 업데이트**

vdmadmin 명령을 -F 옵션과 함께 사용하여 데스크톱을 사용하도록 인증된 Active Directory의 Windows 사용자 외부 보안 주체(FSP)를 업데이트할 수 있습니다.

- **-H 옵션을 사용하여 상태 모니터 나열 및 표시**

vdmadmin 명령을 -H 옵션과 함께 사용하여 기존 상태 모니터를 나열하고, Horizon 7 구성 요소의 인스턴스를 모니터링하고, 특정 상태 모니터나 모니터 인스턴스의 세부 정보를 표시할 수 있습니다.

- **-I 옵션을 사용한 Horizon 7 작업 보고서 나열 및 표시**

vdmadmin 명령을 -I 옵션과 함께 사용해 사용 가능한 Horizon 7 작업 보고서를 나열하고 이들 보고서 가운데 하나의 실행 결과를 표시할 수 있습니다.

- **-l 옵션을 사용하여 Syslog 형식으로 Horizon 7 이벤트 로그 메시지 생성**

vdmadmin 명령에 -l 옵션을 사용하여 이벤트 로그 파일에 Syslog 형식으로 Horizon 7 이벤트 메시지를 기록할 수 있습니다. 많은 타사 분석 제품은 분석 작업을 위한 입력으로 플랫폼 파일 Syslog 데이터를 요구합니다.

- **-L 옵션을 사용하여 전용 시스템 할당**

vdadmin 명령을 -L 옵션과 함께 사용하여 전용 풀의 시스템을 사용자에게 할당할 수 있습니다.

- **-M 옵션을 사용하여 시스템 정보 표시**

vdadmin 명령을 -M 옵션과 함께 사용해 가상 시스템 또는 물리적 컴퓨터의 구성 정보를 표시할 수 있습니다.

- **-M 옵션을 사용하여 가상 시스템의 디스크 공간 회수**

-M 옵션으로 vdadmin 명령을 사용해 연결된 클론 가상 시스템을 디스크 공간 회수 상태로 표시합니다. Horizon 7이 ESXi 호스트에 OS 디스크의 사용되지 않은 공간이 Horizon Administrator에 지정된 최소 임계값에 도달하지 않아도 연결된 클론 OS 디스크의 디스크 공간을 회수하도록 지시합니다.

- **-N 옵션을 사용하여 도메인 필터 구성**

vdadmin 명령을 -N 옵션과 함께 사용하여 Horizon 7가 최종 사용자에게 제공하는 도메인을 제어할 수 있습니다.

- **도메인 필터 구성**

도메인 필터를 적절히 구성해 사용자가 연결 서버 인스턴스 또는 보안 서버를 사용할 수 있는 도메인을 제한할 수 있습니다.

- **-O 및 -P 옵션을 사용하여 권한 없는 사용자의 시스템 및 정책 표시**

vdadmin 명령을 -O 및 -P 옵션과 함께 사용해 더 이상 시스템 사용 권한이 없는 사용자에게 할당된 가상 시스템과 정책을 표시할 수 있습니다.

- **-Q 옵션을 사용하여 키오스크 모드에서 클라이언트 구성**

vdadmin 명령을 -Q 옵션과 함께 사용해 키오스크 모드에서 클라이언트 계정 생성 및 기본값 설정, 해당 클라이언트에 대한 인증 사용 설정, 그리고 클라이언트 구성 정보 표시 작업을 수행할 수 있습니다.

- **-R 옵션을 사용하여 시스템의 첫 번째 사용자 표시**

vdadmin 명령에 -R 옵션을 사용하여 관리되는 가상 시스템의 초기 할당을 확인할 수 있습니다. 예를 들어, LADP 데이터가 손실된 경우 사용자에게 가상 시스템을 다시 할당하려면 이 정보가 필요할 수 있습니다.

- **-S 옵션을 사용하여 연결 서버 인스턴스 또는 보안 서버의 항목 제거**

vdadmin 명령을 -S 옵션과 함께 사용하면 Horizon 7 구성에서 연결 서버 인스턴스 또는 보안 서버의 항목을 제거할 수 있습니다.

- **-T 옵션을 사용하는 관리자에게 보조 자격 증명 제공**

vdadmin 명령을 -T 옵션과 함께 사용하여 관리자에게 Active Directory 보조 자격 증명을 제공할 수 있습니다.

- **-U 옵션을 사용한 사용자 정보 표시**

vdadmin 명령을 -U 옵션과 함께 사용해 사용자 세부 정보를 표시할 수 있습니다.

- **-V 옵션을 사용하여 가상 시스템 잠금 해제 또는 잠금**

vdadmin 명령을 -V 옵션과 함께 사용하여 데이터 센터의 가상 시스템을 잠금 해제하거나 잠글 수 있습니다.

- **-X 옵션을 사용한 LDAP 항목 및 스키마 충돌 감지 및 해결**

vdadmin 명령을 -X 옵션과 함께 사용하여 그룹의 복제된 연결 서버 인스턴스에서 LDAP 항목 충돌 및 LDAP 스키마 충돌을 감지하고 해결할 수 있습니다. 이 옵션을 사용하여 Cloud Pod 아키텍처 환경에서 LDAP 스키마 충돌을 감지하고 해결할 수도 있습니다.

vdadmin 명령 사용

vdadmin 명령 구문은 해당 작업을 제어합니다.

Windows 명령 프롬프트에서 다음 vdadmin 명령 형식을 사용합니다.

```
vdadmin command_option [additional_option argument] ...
```

사용할 수 있는 추가 옵션은 명령 옵션에 따라 다릅니다.

기본적으로 vdadmin 명령 실행 파일의 경로는 C:\Program Files\VMware\VMware

View\Server\Tools\bin입니다. 명령줄에 경로를 입력하지 않으려면 PATH 환경 변수에 경로를 추가하십시오.

- **vdadmin 명령 인증**

vdadmin 명령은 지정된 작업이 성공하도록 **관리자** 역할을 가진 사용자로 실행해야 합니다.

- **vdadmin 명령 출력 형식**

일부 vdadmin 명령 옵션을 사용하여 출력 정보의 형식을 지정할 수 있습니다.

- **vdadmin 명령 옵션**

vdadmin 명령의 명령 옵션을 사용하여 수행할 작업을 지정합니다.

vdadmin 명령 인증

vdadmin 명령은 지정된 작업이 성공하도록 **관리자** 역할을 가진 사용자로 실행해야 합니다.

Horizon Administrator를 사용하여 사용자에게 **관리자** 역할을 할당할 수 있습니다. [장6역할 기반 위임된 관리 구성](#)의 내용을 참조하십시오.

권한이 충분하지 않은 사용자로 로그인할 경우 해당 사용자의 암호를 알면 -b 옵션을 사용하여 **관리자** 역할이 할당되지 않은 사용자로 명령을 실행할 수 있습니다. -b 옵션을 지정하여 지정된 도메인에 지정된 사용자로 vdadmin 명령을 실행할 수 있습니다. 다음 -b 옵션의 사용 형식이 동일합니다.

```
-b username domain [password | *]
```

```
-b username@domain [password | *]
```

```
-b domain\username [password | *]
```

암호 대신에 별표(*)를 지정하면 암호를 입력하라는 메시지가 표시되며, vdmadmin 명령은 명령줄의 명령 기록에 민감한 암호를 남기지 않습니다.

-b 옵션은 -R 및 -T 옵션을 제외한 모든 명령 옵션과 함께 사용할 수 있습니다.

vdmadmin 명령 출력 형식

일부 vdmadmin 명령 옵션을 사용하여 출력 정보의 형식을 지정할 수 있습니다.

다음 표에는 일부 vdmadmin 명령 옵션이 출력 텍스트를 형식 지정하기 위해 제공하는 옵션이 나와 있습니다.

표 12-1. 출력 형식을 선택하기 위한 옵션

옵션	설명
-CSV	쉼표로 구분된 값으로 출력을 형식 지정합니다.
-n	ASCII(UTF-8) 문자를 사용하여 출력을 표시합니다. 이는 쉼표로 구분된 값 및 일반 텍스트 출력을 위해 설정된 기본 문자입니다.
-w	유니코드(UTF-16) 문자를 사용하여 출력을 표시합니다. 이는 XML 출력을 위해 설정된 기본 문자입니다.
-xml	XML으로 출력을 형식 지정합니다.

vdmadmin 명령 옵션

vdmadmin 명령의 명령 옵션을 사용하여 수행할 작업을 지정합니다.

다음 표에는 Horizon 7의 작업을 제어하고 검토하기 위해 vdmadmin 명령에 사용할 수 있는 명령 옵션이 나와 있습니다.

표 12-2. Vdmadmin 명령 옵션

옵션	설명
-A	Horizon Agent에서 로그 파일에 기록하는 정보를 관리합니다. -A 옵션을 사용하여 Horizon Agent 로그 인 구성 의 내용을 참조하십시오. Horizon Agent에서 보고한 IP 주소를 재정의합니다. -A 옵션을 사용하여 IP 주소 재정의 의 내용을 참조하십시오.
-C	연결 서버 그룹의 이름을 설정합니다. GUID-3AD7B00C-43C4-417E-A06B-7251805657D6#GUID-3AD7B00C-43C4-417E-A06B-7251805657D6 의 내용을 참조하십시오.
-F	모든 사용자 또는 지정된 사용자를 위해 Active Directory의 외부 보안 주체(FSP)를 업데이트합니다. -F 옵션을 사용하여 외부 보안 주체 업데이트 의 내용을 참조하십시오.
-H	Horizon 7 서비스에 대한 상태 정보를 표시합니다. -H 옵션을 사용하여 상태 모니터 나열 및 표시 의 내용을 참조하십시오.
-I	Horizon 7 작업에 대한 보고서를 생성합니다. -I 옵션을 사용한 Horizon 7 작업 보고서 나열 및 표시 의 내용을 참조하십시오.
-L	사용자에게 전용 데스크톱을 할당하거나 할당을 제거합니다. -L 옵션을 사용하여 전용 시스템 할당 의 내용을 참조하십시오.

표 12-2. Vdmadmin 명령 옵션 (계속)

옵션	설명
-M	가상 시스템 또는 물리적 컴퓨터에 대한 정보를 표시합니다. -M 옵션을 사용하여 시스템 정보 표시 의 내용을 참조하십시오.
-N	Horizon Client가 사용할 수 있도록 연결 서버 인스턴스 또는 그룹이 제공하는 도메인을 구성합니다. -N 옵션을 사용하여 도메인 필터 구성 의 내용을 참조하십시오.
-O	해당 데스크톱을 더 이상 사용할 권한이 없는 사용자에게 할당된 원격 데스크톱을 표시합니다. -O 및 -P 옵션을 사용하여 권한 없는 사용자의 시스템 및 정책 표시 의 내용을 참조하십시오.
-P	권한 없는 사용자의 원격 데스크톱에 연결된 사용자 정책을 표시합니다. -O 및 -P 옵션을 사용하여 권한 없는 사용자의 시스템 및 정책 표시 의 내용을 참조하십시오.
-Q	Active Directory 계정 및 클라이언트 디바이스의 Horizon 7 구성을 키오스크 모드에서 구성합니다. -Q 옵션을 사용하여 키오스크 모드에서 클라이언트 구성 의 내용을 참조하십시오.
-R	원격 데스크톱에 액세스한 첫 번째 사용자를 보고합니다. -R 옵션을 사용하여 시스템의 첫 번째 사용자 표시 의 내용을 참조하십시오.
-S	Horizon 7 구성에서 연결 서버 인스턴스의 구성 항목을 제거합니다. -S 옵션을 사용하여 연결 서버 인스턴스 또는 보안 서버의 항목 제거 의 내용을 참조하십시오.
-T	관리자에게 Active Directory 보조 자격 증명을 제공합니다. -T 옵션을 사용하는 관리자에게 보조 자격 증명 제공 의 내용을 참조하십시오.
-U	사용자의 원격 데스크톱 권한과 ThinApp 할당 및 관리자 역할을 포함하여 사용자에 대한 정보를 표시합니다. -U 옵션을 사용한 사용자 정보 표시 의 내용을 참조하십시오.
-V	가상 시스템을 잠금거나 잠금을 해제합니다. -V 옵션을 사용하여 가상 시스템 잠금 해제 또는 잠금 의 내용을 참조하십시오.
-X	복제된 연결 서버 인스턴스에서 중복된 LDAP 항목을 검색 및 확인합니다. -X 옵션을 사용한 LDAP 항목 및 스키마 충돌 감지 및 해결 의 내용을 참조하십시오.

-A 옵션을 사용하여 Horizon Agent 로그인 구성

vdmadmin 명령을 -A 옵션과 함께 사용해 Horizon Agent에서 로깅을 구성할 수 있습니다.

구문

```
vdmadmin -A [-b authentication_arguments] -getDCT-outfile local_file -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -getlogfile logfile -outfile local_file -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -getloglevel [-xml] -d desktop [-m machine]
```

```
vdmadmin -A [-b authentication_arguments] -getstatus [-xml] -d desktop [-m machine]
```

```
vdmadmin -A [-b authentication_arguments] -getversion [-xml] -d desktop [-m machine]
```

```
vdmadmin -A [-b authentication_arguments] -list [-xml] [-w | -n] -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -setloglevel level -d desktop [-m machine]
```

사용 정보

DCT(데이터 수집 도구) 번들을 생성해 VMware 기술 지원의 Horizon Agent 문제 해결 작업을 지원할 수 있습니다. 로깅 수준을 변경하고 Horizon Agent의 버전과 상태를 표시하고 로컬 디스크에 개별 로그 파일을 저장할 수도 있습니다.

옵션

다음 표에는 Horizon Agent에서 로깅을 구성하기 위해 지정할 수 있는 옵션이 나와 있습니다.

표 12-3. Horizon Agent의 로그인 구성 옵션

옵션	설명
-d desktop	데스크톱 풀을 지정합니다.
-getDCT	DCT(데이터 수집 도구) 번들을 생성해 로컬 파일에 저장합니다.
-getlogfile logfile	복사본을 저장할 로그 파일 이름을 지정합니다.
-getloglevel	Horizon Agent의 현재 로깅 수준을 표시합니다.
-getstatus	Horizon Agent의 상태를 표시합니다.
-getversion	Horizon Agent의 버전을 표시합니다.
-list	Horizon Agent의 로그 파일을 나열합니다.
-m machine	데스크톱 풀 내에서 시스템을 지정합니다.

표 12-3. Horizon Agent 의 로그인 구성 옵션 (계속)

옵션	설명
-outfile local_file	DCT 번들 또는 로그 파일 복사본을 저장할 로컬 파일 이름을 지정합니다.
-setloglevel level	Horizon Agent의 로깅 수준을 설정합니다.
	디버그 로그 오류, 경고 및 디버깅 이벤트
	보통 로그 오류 및 경고 이벤트
	추적 로그 오류, 경고, 정보 및 디버깅 이벤트

예제

데스크톱 풀 dtpool2의 시스템 machine1에 대한 Horizon Agent 로깅 수준을 표시합니다.

```
vdadmin -A -d dtpool2 -m machine1 -getloglevel
```

데스크톱 풀 dtpool2의 시스템 machine1에 대한 Horizon Agent 로깅 수준을 디버그로 설정합니다.

```
vdadmin -A -d dtpool2 -m machine1 -setloglevel debug
```

데스크톱 풀 dtpool2의 machine1 시스템에 대한 Horizon Agent 로그 파일 목록을 표시합니다.

```
vdadmin -A -d dtpool2 -m machine1 -list
```

데스크톱 풀 dtpool2의 시스템 machine1에 대한 Horizon Agent 로그 파일 log-2009-01-02.txt를 복사해 C:\Wmycopiedlog.txt로 저장합니다.

```
vdadmin -A -d dtpool2 -m machine1 -getlogfile log-2009-01-02.txt -outfile C:\Wmycopiedlog.txt
```

데스크톱 풀 dtpool2의 시스템 machine1에 대한 Horizon Agent의 버전을 표시합니다.

```
vdadmin -A -d dtpool2 -m machine1 -getversion
```

데스크톱 풀 dtpool2의 시스템 machine1에 대한 Horizon Agent의 상태를 표시합니다.

```
vdadmin -A -d dtpool2 -m machine1 -getstatus
```

데스크톱 풀 dtpool2의 시스템 machine1에 대한 DCT 번들을 생성하고 압축 파일 C:\Wmyfile.zip에 작성하십시오.

```
vdadmin -A -d dtpool2 -m machine1 -getDCT -outfile C:\Wmyfile.zip
```

-A 옵션을 사용하여 IP 주소 재정의

vdmadmin 명령을 -A 옵션과 함께 사용하여 Horizon Agent에서 보고한 IP 주소를 재정의할 수 있습니다.

구문

```
vdmadmin -A [-b authentication_arguments] -override -i ip_or_dns -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -override -list -d desktop -m machine
```

```
vdmadmin -A [-b authentication_arguments] -override -r -d desktop [-m machine]
```

사용 정보

Horizon Agent는 실행 중인 시스템에서 검색한 IP 주소를 연결 서버 인스턴스에 보고합니다. 연결 서버 인스턴스가 Horizon Agent에서 보고하는 값을 신뢰할 수 없는 보안 구성에서, Horizon Agent가 제공한 값을 재정의하여 관리된 시스템에서 사용해야 하는 IP 주소를 지정할 수 있습니다. Horizon Agent에서 보고하는 시스템의 주소가 정의된 주소와 일치하지 않는 경우, Horizon Client를 사용하여 시스템에 액세스할 수 없습니다.

옵션

다음 표에는 IP 주소를 재정의하기 위해 지정할 수 있는 옵션이 나와 있습니다.

표 12-4. IP 주소 재정의 옵션

옵션	설명
-d desktop	데스크톱 풀을 지정합니다.
-i ip_or_dns	DNS의 IP 주소 또는 확인 가능한 도메인 이름을 지정합니다.
-m machine	데스크톱 풀의 시스템 이름을 지정합니다.
-override	IP 주소 재정의 작업을 지정합니다.
-r	재정의된 IP 주소를 제거합니다.

예제

데스크톱 풀 dtpool2의 시스템 machine2의 IP 주소를 재정의합니다.

```
vdmadmin -A -override -i 10.20.54.165 -d dtpool2 -m machine2
```

데스크톱 풀 dtpool2의 시스템 machine2에 정의된 IP 주소를 표시합니다.

```
vdadmin -A -override -list -d dtpool2 -m machine2
```

데스크톱 풀 dtpool2의 시스템 machine2에 정의된 IP 주소를 제거합니다.

```
vdadmin -A -override -r -d dtpool2 -m machine2
```

데스크톱 풀 dtpool3의 데스크톱에 정의된 IP 주소를 제거합니다.

```
vdadmin -A -override -r -d dtpool3
```

-F 옵션을 사용하여 외부 보안 주체 업데이트

vdadmin 명령을 -F 옵션과 함께 사용하여 데스크톱을 사용하도록 인증된 Active Directory의 Windows 사용자 외부 보안 주체(FSP)를 업데이트할 수 있습니다.

구문

```
vdadmin -F [-b authentication_arguments] [-u domain\user]
```

사용 정보

로컬 도메인의 외부 도메인을 신뢰할 경우, 로컬 도메인 리소스에 대한 외부 도메인의 보안 주체로 액세스할 수 있습니다. Active Directory는 FSP를 사용하여 신뢰된 외부 도메인의 보안 주체를 나타냅니다. 신뢰된 외부 도메인의 목록을 수정할 경우 사용자의 FSP를 업데이트할 수 있습니다.

옵션

-u 옵션은 FSP를 업데이트할 사용자의 이름 및 도메인을 지정합니다. 이 옵션을 지정하지 않을 경우, 명령은 Active Directory의 모든 사용자 FSP를 업데이트합니다.

예

EXTERNAL 도메인 사용자 Jim의 FSP를 업데이트합니다.

```
vdadmin -F -u EXTERNAL\Jim
```

Active Directory의 모든 사용자 FSP를 업데이트합니다.

```
vdadmin -F
```

-H 옵션을 사용하여 상태 모니터 나열 및 표시

vdmadmin 명령을 -H 옵션과 함께 사용하여 기존 상태 모니터를 나열하고, Horizon 7 구성 요소의 인스턴스를 모니터링하고, 특정 상태 모니터나 모니터 인스턴스의 세부 정보를 표시할 수 있습니다.

구문

```
vdmadmin -H [-b authentication_arguments] -list -xml [-w | -n]
```

```
vdmadmin -H [-b authentication_arguments] -list -monitorid monitor_id -xml [-w | -n]
```

```
vdmadmin -H [-b authentication_arguments] -monitorid monitor_id -instanceid instance_id -xml [-w | -n]
```

사용 정보

다음 표에는 Horizon 7에서 구성 요소의 상태를 모니터링하는 데 사용하는 상태 모니터가 나와 있습니다.

표 12-5. 상태 모니터

모니터	설명
CBMonitor	연결 서버 인스턴스의 상태를 모니터링합니다.
DBMonitor	이벤트 데이터베이스의 상태를 모니터링합니다.
DomainMonitor	연결 서버 호스트의 로컬 도메인과 신뢰할 수 있는 모든 도메인 상태를 모니터링합니다.
SGMonitor	보안 게이트웨이 서비스와 보안 서버의 상태를 모니터링합니다.
VCMonitor	vCenter 서버의 상태를 모니터링합니다.

구성 요소의 인스턴스가 여러 개 있는 경우 Horizon 7는 구성 요소의 인스턴스 각각을 모니터링하는 개별 모니터 인스턴스를 생성합니다.

이 명령을 통해 상태 모니터와 모니터 인스턴스에 대한 모든 정보를 XLM 형식으로 출력할 수 있습니다.

옵션

다음 표에는 상태 모니터를 나열하고 표시할 때 지정할 수 있는 옵션이 나와 있습니다.

표 12-6. 상태 모니터 나열 및 표시 옵션

옵션	설명
-instanceid instance_id	상태 모니터 인스턴스를 지정합니다.
-list	상태 모니터 ID가 지정되지 않은 경우 기존 상태 모니터를 표시합니다.

표 12-6. 상태 모니터 나열 및 표시 옵션 (계속)

옵션	설명
<code>-list -monitorid monitor_id</code>	지정된 상태 모니터 ID에 대한 모니터 인스턴스를 표시합니다.
<code>-monitorid monitor_id</code>	상태 모니터 ID를 지정합니다.

예제

유니코드 문자를 사용해 모든 기존 상태 모니터를 XML 형식으로 나열하십시오.

```
vdadmin -H -list -xml
```

ASCII 문자를 사용해 vCenter 모니터(VCMonitor)의 모든 인스턴스를 XML 형식으로 나열하십시오.

```
vdadmin -H -list -monitorid VCMonitor -xml -n
```

지정된 vCenter 모니터 인스턴스의 상태를 표시하십시오.

```
vdadmin -H -monitorid VCMonitor -instanceid 4aec2c99-4879-96b2-de408064d035 -xml
```

-l 옵션을 사용한 Horizon 7 작업 보고서 나열 및 표시

vdadmin 명령을 -l 옵션과 함께 사용해 사용 가능한 Horizon 7 작업 보고서를 나열하고 이들 보고서 가운데 하나의 실행 결과를 표시할 수 있습니다.

구문

```
vdadmin -l [-b authentication_arguments] -list [-xml] [-w | -n]
```

```
vdadmin -l [-b authentication_arguments] -report report -view view [-startdate yyyy-MM-dd-HH:mm:ss][-enddate yyyy-MM-dd-HH:mm:ss] [-w | -n] -xml | -csv
```

사용 정보

이 명령을 사용해 사용 가능한 보고서와 보기를 표시하고 Horizon 7에서 지정한 보고서 및 보기에 대해 기록한 정보를 표시할 수 있습니다.

vdadmin 명령을 -l 옵션과 함께 사용해 syslog 형식으로 Horizon 7 로그 메시지를 생성할 수도 있습니다. [-l 옵션을 사용하여 Syslog 형식으로 Horizon 7 이벤트 로그 메시지 생성의 내용을 참조하십시오.](#)

옵션

다음 표에는 보고서 및 보기를 나열하고 표시할 때 지정할 수 있는 옵션이 나와 있습니다.

표 12-7. 보고서 및 보기 나열 및 표시 옵션

옵션	설명
-enddate yyyy-MM-dd-HH:mm:ss	표시되는 정보 날짜에 대한 상한값을 지정합니다.
-list	사용할 수 있는 보고서 및 보기를 나열합니다.
-report report	보고서를 지정합니다.
-startdate yyyy-MM-dd-HH:mm:ss	표시되는 정보 날짜에 대한 하한값을 지정합니다.
-view view	보기를 지정합니다.

예제

유니코드 문자를 사용해 사용할 수 있는 보고서와 보기를 XML 형식으로 나열하십시오.

```
vdadmin -l -list -xml -w
```

ASCII 문자를 사용해 2010년 8월 1일 이후 발생한 사용자 이벤트 목록을 쉼표로 구분된 값으로 표시하십시오.

```
vdadmin -l -report events -view user_events -startdate 2010-08-01-00:00:00 -csv -n
```

-l 옵션을 사용하여 Syslog 형식으로 Horizon 7 이벤트 로그 메시지 생성

vdadmin 명령에 -l 옵션을 사용하여 이벤트 로그 파일에 Syslog 형식으로 Horizon 7 이벤트 메시지를 기록할 수 있습니다. 많은 타사 분석 제품은 분석 작업을 위한 입력으로 플랫폼 파일 Syslog 데이터를 요구합니다.

구문

```
vdadmin -l -eventSyslog -disable
```

```
vdadmin -l -eventSyslog -enable -localOnly
```

```
vdadmin -l -eventSyslog -enable -path path
```

```
vdadmin -l -eventSyslog -enable -path path  
-user DomainName\Username -password password
```

사용 정보

이 명령을 사용하여 Syslog 형식으로 Horizon 7 이벤트 로그 메시지를 생성할 수 있습니다. Syslog 파일에서 Horizon 7 이벤트 로그 메시지는 분석 소프트웨어에서 로깅 데이터를 액세스할 수 있도록 키 값 쌍으로 서식이 지정됩니다.

또한 -l 옵션으로 vdmadmin 명령을 사용해 사용 가능한 보고서와 보기를 나열하고 지정된 보고서의 내용을 표시할 수 있습니다. [-l 옵션을 사용한 Horizon 7 작업 보고서 나열 및 표시](#)의 내용을 참조하십시오.

옵션

eventSyslog 옵션을 사용하도록 또는 사용하지 않도록 설정할 수 있습니다. Syslog 출력을 로컬 시스템으로만 보내거나 다른 위치로 보낼 수 있습니다. Horizon 7 5.2 이상에서는 Syslog 서버에 UDP를 직접 연결할 수 있습니다. Horizon 7 설치 문서에서 "Syslog 서버의 이벤트 로깅 구성"을 참조하십시오.

표 12-8. Syslog 형식으로 Horizon 7 이벤트 로그 메시지를 생성할 수 있는 옵션

옵션	설명
-disable	Syslog 로깅을 사용하지 않도록 설정합니다.
-e -enable	Syslog 로깅을 사용하도록 설정합니다.
-eventSyslog	Horizon 7 이벤트를 Syslog 형식으로 생성하도록 지정합니다.
-localOnly	Syslog 출력을 로컬 시스템에만 저장합니다. -localOnly 옵션을 사용할 경우 Syslog 출력의 기본 대상은 %PROGRAMDATA%\VMware\WDDM\Events입니다.
-password password	Syslog 출력의 지정된 대상 경로에 대한 액세스를 승인하는 사용자의 암호를 지정합니다.
-path	Syslog 출력의 대상 UNC 경로를 결정합니다.
-u -user DomainName\username	Syslog 출력의 대상 경로에 액세스할 수 있는 도메인과 사용자 이름을 지정합니다.

예제

Horizon 7 이벤트를 Syslog 형식으로 생성하지 않도록 지정합니다.

```
vdmadmin -l -eventSyslog -disable
```

Horizon 7 이벤트의 Syslog 출력을 로컬 시스템에만 보냅니다.

```
vdmadmin -l -eventSyslog -enable -localOnly
```

Horizon 7 이벤트의 직접 Syslog 출력을 지정한 경로로 보냅니다.

```
vdmadmin -l -eventSyslog -enable -path path
```

Horizon 7 이벤트의 직접 Syslog 출력을 권한 있는 도메인 사용자만 액세스할 수 있는 지정된 경로로 보냅니다.

```
vdmadmin -l -eventSyslog -enable -path \\logserver\share\ViewEvents -user mydomain\myuser  
-password mypassword
```


-L 옵션을 사용하여 전용 시스템 할당

vdadmin 명령을 -L 옵션과 함께 사용하여 전용 풀의 시스템을 사용자에게 할당할 수 있습니다.

구문

```
vdadmin -L [-b authentication_arguments] -d desktop -m machine -u domain\user
```

```
vdadmin -L [-b authentication_arguments] -d desktop [-m machine | -u domain\user] -r
```

사용 정보

Horizon 7는 사용자가 전용 데스크톱 풀에 처음 연결할 때 시스템을 할당합니다. 경우에 따라서는 사용자에게 시스템을 미리 할당해야 할 수 있습니다. 예를 들어, 사용자가 처음 연결하기 전에 사용자의 시스템 환경을 준비할 수 있습니다. Horizon 7이 전용 풀에서 할당한 원격 데스크톱에 사용자가 연결하면, 해당 데스크톱을 호스트하는 가상 시스템은 가상 시스템의 수명 동안 같은 사용자에게 할당된 채로 남아 있습니다. 전용 풀의 가상 시스템 하나에 사용자를 할당할 수 있습니다.

시스템은 권한을 가진 임의의 사용자에게 할당할 수 있습니다. 연결 서버 인스턴스에서 View LDAP 데이터 손실을 복원할 때 또는 특정 시스템의 소유권을 변경할 때 이러한 작업을 수행할 수 있습니다.

Horizon 7가 전용 풀에서 할당한 원격 데스크톱에 사용자가 연결하면, 해당 원격 데스크톱은 데스크톱을 호스트하는 가상 시스템의 수명 동안 같은 사용자에게 할당된 채로 남아 있습니다. 조직을 떠난 사용자, 더 이상 데스크톱 액세스 권한이 필요 없는 사용자 또는 다른 데스크톱 풀의 데스크톱을 사용할 사용자의 시스템 할당을 제거할 수 있습니다. 또한 데스크톱에 액세스하는 모든 사용자의 할당을 제거할 수 있습니다.

참고 vdadmin -L 명령은 View Composer 영구 디스크에 소유권을 할당하지 않습니다. 영구 디스크가 있는 연결된 클론 데스크톱을 사용자에게 할당하려면 Horizon Administrator에서 **사용자 할당** 메뉴 옵션을 사용합니다.

vdadmin -L을 사용하여 영구 디스크를 연결한 연결된 클론 데스크톱을 사용자에게 할당하면 특정 상황에서 예기치 않은 결과가 발생할 수 있습니다. 예를 들어, 영구 디스크를 분리하고 이를 사용해 데스크톱을 생성하면 생성된 데스크톱이 원래 데스크톱의 소유자에게 할당되지 않습니다.

옵션

다음 표에는 사용자에게 데스크톱을 할당하거나 할당을 제거할 때 지정할 수 있는 옵션이 나와 있습니다.

표 12-9. 전용 데스크톱 할당 옵션

옵션	설명
-d desktop	데스크톱 풀 이름을 지정합니다.
-m machine	원격 데스크톱을 호스트하는 가상 시스템의 이름을 지정합니다.

표 12-9. 전용 데스크톱 할당 옵션 (계속)

옵션	설명
-r	특정 사용자에게 대한 할당 또는 특정 시스템에 대한 모든 할당을 제거합니다.
-u domain\user	사용자의 도메인과 로그인 이름을 지정합니다.

예제

CORP 도메인의 사용자 Jo에게 데스크톱 풀 dtpool1의 시스템 machine2를 할당하십시오.

```
vdmadmin -L -d dtpool1 -m machine2 -u CORP\Jo
```

풀 dtpool1의 데스크톱에서 CORP 도메인의 사용자 Jo에 대한 할당을 제거하십시오.

```
vdmadmin -L -d dtpool1 -u Corp\Jo -r
```

데스크톱 풀 dtpool3의 시스템 machine1에서 모든 사용자 할당을 제거하십시오.

```
vdmadmin -L -d dtpool3 -m machine1 -r
```

-M 옵션을 사용하여 시스템 정보 표시

vdmadmin 명령을 -M 옵션과 함께 사용해 가상 시스템 또는 물리적 컴퓨터의 구성 정보를 표시할 수 있습니다.

구문

```
vdmadmin -M [-b authentication_arguments] [-m machine | [-u domain\user]][-d desktop]] [-xml | -csv] [-w | -n]
```

사용 정보

이 명령은 원격 데스크톱의 기본 가상 시스템 또는 물리적 컴퓨터에 대한 정보를 표시합니다.

- 시스템의 디스플레이 이름
- 데스크톱 풀 이름
- 시스템 상태

시스템 상태는 UNDEFINED, PRE_PROVISIONED, CLONING, CLONINGERROR, CUSTOMIZING, READY, DELETING, MAINTENANCE, ERROR, LOGOUT 값 중 하나일 수 있습니다.

이 명령은 연결된 또는 연결 끊김 등 Horizon Administrator에 표시되는 모든 동적 시스템 상태를 표시하지는 않습니다.

- 할당된 사용자의 SID
- 할당된 사용자의 계정 이름

- 할당된 사용자의 도메인 이름
- 가상 시스템의 인벤토리 경로(해당되는 경우)
- 시스템 생성 날짜
- 시스템의 템플릿 경로(해당되는 경우)
- vCenter Server의 URL(해당되는 경우)

옵션

다음 표에는 상세 정보를 표시할 가상 시스템을 지정할 때 사용할 수 있는 옵션이 나와 있습니다.

표 12-10. 시스템 정보 표시 옵션

옵션	설명
-d desktop	데스크톱 풀 이름을 지정합니다.
-m machine	가상 시스템 이름을 지정합니다.
-u domain\user	사용자의 도메인과 로그인 이름을 지정합니다.

예제

CORP 도메인에서 사용자 Jo에게 할당된 dtpool2 풀의 원격 데스크톱에 대한 기본 시스템 정보를 표시하고 ASCII 문자를 사용해 출력 형식을 XML로 지정하십시오.

```
vdmadmin -M -u CORPWJo -d dtpool2 -xml -n
```

machine3 시스템에 대한 정보를 표시하고 쉼표로 구분된 값으로 출력 형식을 지정하십시오.

```
vdmadmin -M -m machine3 -csv
```

-M 옵션을 사용하여 가상 시스템의 디스크 공간 회수

-M 옵션으로 vdmadmin 명령을 사용해 연결된 클론 가상 시스템을 디스크 공간 회수 상태로 표시합니다. Horizon 7이 ESXi 호스트에 OS 디스크의 사용되지 않은 공간이 Horizon Administrator에 지정된 최소 임계값에 도달하지 않아도 연결된 클론 OS 디스크의 디스크 공간을 회수하도록 지시합니다.

구문

```
vdmadmin -M [-b authentication_arguments] -d desktop -m machine -markForSpaceReclamation
```

사용 정보

이 옵션을 사용하면 시연 또는 문제 해결을 위해 특정 가상 시스템에서 디스크 공간 회수를 시작할 수 있습니다.

블랙아웃 기간이 적용 중일 때 이 명령을 실행하면 공간 회수가 발생하지 않습니다.

-M 옵션으로 vdmadmin 명령을 사용하여 디스크 공간을 사용하려면 다음 전제 조건을 충족해야 합니다.

- Horizon 7이 vCenter Server 및 ESXi 버전 5.1 이상을 사용하고 있는지 확인합니다.
- vSphere 버전 5.1 이상에서 제공되는 VMware Tools가 가상 시스템에 설치되어 있는지 확인합니다.
- 가상 시스템의 가상 하드웨어 버전이 9 이상인지 확인합니다.
- Horizon Administrator에서 vCenter Server에 **공간 회수를 사용하도록 설정** 옵션이 선택되었는지 확인합니다. **vSphere가 연결된 클론 가상 시스템의 디스크 공간을 회수할 수 있도록 허용**을 참조하십시오.
- Horizon Administrator에서 데스크톱 풀에 **VM 디스크 공간 회수** 옵션이 선택되었는지 확인합니다. Horizon 7에서 가상 데스크톱 설정 문서에서 "View Composer 연결된 클론에서 디스크 공간 회수"를 참조하십시오.
- 공간 회수 작업을 시작하기 전에 가상 시스템의 전원이 켜져 있는지 확인합니다.
- 블랙아웃 기간이 적용되고 있지 않은지 확인합니다. Horizon 7에서 가상 데스크톱 설정 문서에서 "View Composer 연결된 클론의 Storage Accelerator 및 공간 회수 블랙아웃 횃수 설정"을 참조하십시오.

옵션

표 12-11. 가상 시스템의 디스크 공간을 회수할 수 있는 옵션

옵션	설명
-d desktop	데스크톱 풀 이름을 지정합니다.
-m machine	가상 시스템 이름을 지정합니다.
-MarkForSpaceReclamation	가상 시스템을 디스크 공간 회수 상태로 표시합니다.

예

데스크톱 풀 pool1의 가상 시스템 machine3을 디스크 공간 회수 상태로 표시합니다.

```
vdmadmin -M -d pool1 -m machine3 -markForSpaceReclamation
```

-N 옵션을 사용하여 도메인 필터 구성

vdmadmin 명령을 -N 옵션과 함께 사용하여 Horizon 7가 최종 사용자에게 제공하는 도메인을 제어할 수 있습니다.

구문

```
vdmadmin -N [-b authentication_arguments] -domains {-exclude | -include | -search} -domain domain -add [-s connsvr]
```

```
vdmadmin -N [-b authentication_arguments] -domains -list [-w | -n] [-xml]
```

```
vdmadmin -N [-b authentication_arguments] -domains -list -active [-w | -n] [-xml]
```

```
vdmadmin -N [-b authentication_arguments] -domains {-exclude | -include | -search} -domain domain -remove [-s connsvr]
```

```
vdmadmin -N [-b authentication_arguments] -domains {-exclude | -include | -search} -removeall [-s connsvr]
```

사용 정보

제외 목록, 포함 목록, 검색 제외 목록에 각각 작업을 적용하려면 `-exclude`, `-include`, 또는 `-search` 옵션 중 하나를 지정하십시오.

검색 제외 목록에 도메인을 추가하면 자동 도메인 검색에서 해당 도메인이 제외됩니다.

포함 목록에 도메인을 추가하면 검색 결과에 해당 도메인이 포함됩니다.

제외 목록에 도메인을 추가하면 검색 결과에서 해당 도메인이 제외됩니다.

옵션

다음 표에는 도메인 필터를 구성하기 위해 지정할 수 있는 옵션이 나와 있습니다.

표 12-12. 도메인 필터 구성 옵션

옵션	설명
<code>-add</code>	목록에 도메인을 추가합니다.
<code>-domain domain</code>	필터링할 도메인을 지정합니다. DNS 이름이 아닌 NetBIOS 이름으로 도메인을 지정해야 합니다.
<code>-domains</code>	도메인 필터 작업을 지정합니다.
<code>-exclude</code>	제외 목록 작업을 지정합니다.
<code>-include</code>	포함 목록 작업을 지정합니다.
<code>-list</code>	각 연결 서버 인스턴스 및 연결 서버 그룹에서 검색 제외 목록, 제외 목록, 포함 목록에 구성된 도메인을 표시합니다.
<code>-list -active</code>	명령을 실행하는 연결 서버 인스턴스에 대해 사용할 수 있는 도메인을 표시합니다.
<code>-remove</code>	목록에서 도메인을 제거합니다.
<code>-removeall</code>	목록에서 모든 도메인을 제거합니다.

표 12-12. 도메인 필터 구성 옵션 (계속)

옵션	설명
-s connsvr	연결 서버 인스턴스의 도메인 필터에 적용하는 작업을 지정합니다. 이름 또는 IP 주소로 연결 서버 인스턴스를 지정할 수 있습니다. 이 옵션을 지정하지 않으면 검색 구성의 모든 변경 사항이 그룹의 모든 연결 서버 인스턴스에 적용됩니다.
-search	검색 제외 목록 작업을 지정합니다.

예제

연결 서버 인스턴스 csvr1의 검색 제외 목록에 도메인 FARDOM을 추가하십시오.

```
vdmadmin -N -domains -search -domain FARDOM -add -s csvr1
```

연결 서버 그룹의 제외 목록에 도메인 NEARDOM을 추가하십시오.

```
vdmadmin -N -domains -exclude -domain NEARDOM -add
```

그룹의 연결 서버 인스턴스 및 그룹의 도메인 검색 구성을 표시하십시오.

```
C:\W vdmadmin -N -domains -list
```

```
Domain Configuration
```

```
=====
```

```
Cluster Settings
```

```
Include:
```

```
Exclude:
```

```
Search :
```

```
FARDOM
```

```
DEPTX
```

```
Broker Settings: CONSVR-1
```

```
Include:
```

```
(*)Exclude:
```

```
YOURDOM
```

```
Search :
```

```
Broker Settings: CONSVR-2
```

```
Include:
```

```
Exclude:
```

```
Search :
```

Horizon 7은 FARDOM 도메인과 DEPTX 도메인을 제외하도록 그룹의 각 연결 서버 호스트에 대한 도메인 검색을 제한합니다. CONSVR-1의 제외 목록 옆에 있는 문자(*)는 Horizon 7가 CONSVR-1에 대한 도메인 검색 결과에서 YOURDOM 도메인을 제외한다는 것을 나타냅니다.

ASCII 문자를 사용해 XML 형식으로 도메인 필터를 표시하십시오.

```
vdmadmin -N -domains -list -xml -n
```

로컬 연결 서버 인스턴스에서 Horizon 7이 사용할 수 있는 도메인을 표시합니다.

```
C:\W vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: FARDOM DNS:fardom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

```
Domain: DEPTY DNS:depty.mycorp.com
```

```
Domain: DEPTZ DNS:deptz.mycorp.com
```

ASCII 문자를 사용해 XML 형식으로 사용할 수 있는 도메인을 표시하십시오.

```
vdmadmin -N -domains -list -active -xml -n
```

연결 서버 그룹의 제외 목록에서 도메인 NEARDOM을 제거하십시오.

```
vdmadmin -N -domains -exclude -domain NEARDOM -remove
```

연결 서버 인스턴스 csvr1의 포함 목록에서 모든 도메인을 제거하십시오.

```
vdmadmin -N -domains -include -removeall -s csvr1
```

도메인 필터 구성

도메인 필터를 적절히 구성해 사용자가 연결 서버 인스턴스 또는 보안 서버를 사용할 수 있는 도메인을 제한할 수 있습니다.

Horizon 7은 연결 서버 인스턴스 또는 보안 서버가 속해 있는 도메인부터 신뢰 관계를 탐색하여 어느 도메인에 액세스할 수 있는지 확인합니다. 규모가 작고 연결 관계가 잘 형성되어 있는 도메인의 경우 Horizon 7가 도메인 전체 목록을 신속하게 파악할 수 있지만 도메인 수가 증가하거나 도메인 간 연결 관계가 감소할수록 이러한 작업 시간이 길어집니다. Horizon 7의 검색 결과에는 사용자가 원격 데스크톱에 로그인할 때 제공할 수 없는 도메인도 포함될 수 있습니다.

이전에 재귀적 도메인 열거(HKEY_LOCAL_MACHINE\SOFTWARE\VMware, Inc.\VMware

VDMMRecursiveDomainEnum)를 제어하는 Windows 레지스트리 키 값을 false로 설정한 경우에는 재귀적 도메인 검색을 사용할 수 없고 연결 서버 인스턴스가 주 도메인만 사용합니다. 도메인 필터링 기능을 사용하려면 레지스트리 키를 삭제하거나 레지스트리 키 값을 true로 설정하고 시스템을 다시 시작하십시오. 이 키를 설정한 모든 연결 서버 인스턴스에서 이를 수행해야 합니다.

다음 표에는 도메인 필터 구성 시 지정할 수 있는 도메인 목록 유형이 나와 있습니다.

표 12-13. 도메인 목록 유형

도메인 목록 유형	설명
검색 제외 목록	자동 검색을 수행하는 동안 Horizon 7가 탐색할 수 있는 도메인을 지정합니다. 검색 시 검색 제외 목록에 포함되어 있는 도메인은 무시하고 제외된 도메인이 신뢰하는 도메인은 찾지 않습니다. 주 도메인을 검색에서 제외할 수 없습니다.
제외 목록	Horizon 7이 도메인 검색 결과에서 제외할 도메인을 지정합니다. 주 도메인을 제외할 수 없습니다.
포함 목록	Horizon 7가 도메인 검색 결과에서 제외하지 않을 도메인을 지정합니다. 주 도메인을 제외한 다른 모든 도메인이 제거됩니다.

검색 제외 목록에 지정한 도메인과 이들 제외 도메인이 신뢰하는 도메인을 제외한 도메인 목록을 자동 도메인 검색에서 검색합니다. Horizon 7은 다음 순서에 따라 비어 있지 않은 제외 목록 또는 포함 목록을 선택합니다.

- 1 연결 서버 인스턴스에 대해 구성된 제외 목록
- 2 연결 서버 그룹에 대해 구성된 제외 목록
- 3 연결 서버 인스턴스에 대해 구성된 포함 목록
- 4 연결 서버 그룹에 대해 구성된 포함 목록

Horizon 7는 선택한 첫 번째 목록만 검색 결과에 적용합니다.

포함하도록 선택한 도메인의 도메인 컨트롤러에 현재 액세스할 수 없는 경우 Horizon 7는 해당 도메인을 활성 도메인 목록에 포함하지 않습니다.

연결 서버 인스턴스 또는 보안 서버에 속해 있는 주 도메인은 제외할 수 없습니다.

도메인을 포함할 필터링 예

포함 목록을 사용하여 Horizon 7가 도메인 검색 결과에서 제외하지 않을 도메인을 지정할 수 있습니다. 주 도메인을 제외한 다른 모든 도메인이 제거됩니다.

연결 서버 인스턴스가 주 MYDOM 도메인에 연결되어 있고 YOURDOM 도메인과 신뢰할 수 있는 관계에 있습니다. YOURDOM 도메인은 DEPTX 도메인과 신뢰할 수 있는 관계에 있습니다.

연결 서버 인스턴스에 대해 현재 활성화되어 있는 도메인을 표시하십시오.

```
C:\W vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
Domain: YOURDOM DNS:yourdom.mycorp.com
Domain: FARDOM DNS: fardom.mycorp.com
Domain: DEPTX DNS:deptx.mycorp.com
Domain: DEPTY DNS:depty.mycorp.com
Domain: DEPTZ DNS:deptz.mycorp.com
```


DEPTY 및 DEPTZ 도메인은 DEPTX 도메인의 신뢰할 수 있는 도메인이기 때문에 목록에 표시됩니다.

연결 서버 인스턴스가 주 MYDOM 도메인 외에 YOURDOM 및 DEPTX 도메인만 사용할 수 있도록 지정하십시오.

```
vdadmin -N -domains -include -domain YOURDOM -add
vdadmin -N -domains -include -domain DEPTX -add
```

YOURDOM 및 DEPTX 도메인을 포함한 후에 현재 활성화되어 있는 도메인을 표시하십시오.

```
C:\W vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

Horizon 7는 도메인 검색 결과에 포함 목록을 적용합니다. 도메인 계층 구조가 매우 복잡하거나 일부 도메인에 대한 네트워크 연결이 안 좋으면 도메인 검색 속도가 느릴 수 있습니다. 이런 경우에는 검색 제외 목록을 대신 사용하십시오.

도메인을 제외할 필터링 예

제외 목록을 사용해 Horizon 7이 도메인 검색 결과에서 제외할 도메인을 지정할 수 있습니다.

연결 서버 인스턴스 그룹 CONSVR-1과 CONSVR-2가 주 MYDOM 도메인에 연결되어 있고 YOURDOM 도메인과 신뢰할 수 있는 관계에 있습니다. YOURDOM 도메인은 DEPTX 및 FARDOM 도메인과 신뢰할 수 있는 관계에 있습니다.

FARDOM 도메인은 지리적으로 멀리 떨어져 있고 도메인의 네트워크 연결 속도가 느리고 대기 시간이 깁니다. FARDOM 도메인의 사용자가 MYDOM 도메인의 연결 서버 그룹에 액세스할 수 있기 위해 필요한 요구 사항은 없습니다.

연결 서버 그룹 구성원에 대해 현재 활성화되어 있는 도메인을 표시하십시오.

```
C:\W vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR-1)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: FARDOM DNS: fardom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

```
Domain: DEPTY DNS:depty.mycorp.com
```

```
Domain: DEPTZ DNS:deptz.mycorp.com
```

DEPTY 및 DEPTZ 도메인은 DEPTX 도메인의 신뢰할 수 있는 도메인입니다.

Horizon Client의 연결 성능을 향상하려면 연결 서버 그룹의 검색 작업에서 FARDOM 도메인을 제외하십시오.

```
vdmadmin -N -domains -search -domain FARDOM -add
```

검색에서 FARDOM 도메인을 제외한 후 현재 활성화되어 있는 도메인을 표시하는 명령입니다.

```
C:\W vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR-1)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

```
Domain: DEPTX DNS:deptx.mycorp.com
```

```
Domain: DEPTY DNS:depty.mycorp.com
```

```
Domain: DEPTZ DNS:deptz.mycorp.com
```

그룹의 모든 연결 서버 인스턴스에 대한 도메인 검색 작업에서 DEPTX 도메인과 이 도메인이 신뢰할 수 있는 모든 도메인을 제외하려면 검색 제외 목록을 확대하십시오. 또한 CONSVR-1에서 사용할 수 있는 도메인에서 YOURDOM 도메인을 제외하십시오.

```
vdmadmin -N -domains -search -domain DEPTX -add
vdmadmin -N -domains -exclude -domain YOURDOM -add -s CONSVR-1
```

새 도메인 검색 구성을 표시하십시오.

```
C:\W vdmadmin -N -domains -list
```

```
Domain Configuration
```

```
=====
```

```
Cluster Settings
```

```
Include:
```

```
Exclude:
```

```
Search :
```

```
FARDOM
```

```
DEPTX
```

```
Broker Settings: CONSVR-1
```

```
Include:
```

```
(*)Exclude:
```

```
YOURDOM
```

```
Search :
```

```
Broker Settings: CONSVR-2
```

```
Include:
```

```
Exclude:
```

```
Search :
```

Horizon 7은 FARDOM 도메인과 DEPTX 도메인을 제외하도록 그룹의 각 연결 서버 호스트에 대한 도메인 검색을 제한합니다. CONSVR-1의 제외 목록 옆에 있는 문자(*)는 Horizon 7가 CONSVR-1에 대한 도메인 검색 결과에서 YOURDOM 도메인을 제외한다는 것을 나타냅니다.

CONSVR-1에서 현재 활성화되어 있는 도메인을 표시하십시오.

```
C:\W vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR-1)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

CONSVR-2에서 현재 활성화되어 있는 도메인을 표시하십시오.

```
C:\W vdmadmin -N -domains -list -active
```

```
Domain Information (CONSVR-2)
```

```
=====
```

```
Primary Domain: MYDOM
```

```
Domain: MYDOM DNS:mydom.mycorp.com
```

```
Domain: YOURDOM DNS:yourdom.mycorp.com
```

-O 및 -P 옵션을 사용하여 권한 없는 사용자의 시스템 및 정책 표시

vdmadmin 명령을 -O 및 -P 옵션과 함께 사용해 더 이상 시스템 사용 권한이 없는 사용자에게 할당된 가상 시스템과 정책을 표시할 수 있습니다.

구문

```
vdmadmin -O [-b authentication_arguments] [-ld | -lu] [-w | -n] [-xml [-noxsIt | -xsIt path path]]
```

```
vdmadmin -P [-b authentication_arguments] [-ld | -lu] [-w | -n] [-xml [-noxsIt | -xsIt path path]]
```

사용 정보

영구 가상 시스템 또는 물리적 시스템에 대한 사용자 권한을 해지해도 연결된 원격 데스크톱 할당이 자동으로 해지되지 않습니다. 이는 사용자 계정을 일시 중단하거나 사용자가 휴직 중일 때 사용할 수 있는 조건입니다. 권한을 다시 사용하도록 설정하면 사용자는 이전과 동일한 가상 시스템을 계속 사용할 수 있습니다. 사용자가 조직을 나가면 다른 사용자가 해당 가상 시스템에 액세스할 수 없으므로 분리해야 하는 경우가 있습니다. 권한 없는 사용자에게 할당된 모든 정책을 검토하는 경우도 있습니다.

옵션

다음 표에는 권한 없는 사용자의 가상 시스템 및 정책을 표시할 때 지정할 수 있는 옵션이 나와 있습니다.

표 12-14. 권한 없는 사용자의 시스템 및 정책 표시 옵션

옵션	설명
-ld	시스템별로 출력 항목을 정렬합니다.
-lu	사용자별로 출력 항목을 정렬합니다.
-noxslt	XML 출력에 기본 스타일시트를 적용하지 않도록 지정합니다.
-xslt path path	XML 출력 변환 시 사용하는 스타일시트 경로를 지정합니다.

표 12-15에서는 XML 출력을 HTML로 변환할 때 적용할 수 있는 스타일시트를 보여줍니다. 스타일시트는 C:\Program Files\VMware\VMware View\server\wetc 디렉토리에 위치합니다.

표 12-15. XSL 스타일시트

스타일시트 파일 이름	설명
unentitled-machines.xsl	현재 사용자에게 할당된 권한 없는 가상 시스템을 사용자 또는 시스템별로 그룹화한 목록을 포함하는 보고서를 변환합니다. 기본 스타일시트입니다.
unentitled-policies.xsl	권한 없는 사용자에게 적용되는 사용자 수준 정책과 함께 가상 시스템 목록을 포함하는 보고서를 변환합니다.

예제

권한 없는 사용자에게 할당된 가상 시스템을 가상 시스템별로 그룹화해 텍스트 형식으로 표시합니다.

```
vdadmin -0 -ld
```

권한 없는 사용자에게 할당된 가상 시스템을 사용자별로 그룹화해 ASCII 문자를 사용해 XML 형식으로 표시합니다.

```
vdadmin -0 -lu -xml -n
```

고유한 스타일시트 C:\tmp\unentitled-users.xsl을 적용하고 uu-output.html 파일로 출력을 리디렉션합니다.

```
vdadmin -0 -lu -xml -xslt path "C:\tmp\unentitled-users.xsl" > uu-output.html
```

권한 없는 사용자의 가상 시스템과 관련된 사용자 정책을 데스크톱별로 그룹화해 유니코드 문자를 사용해 XML 형식으로 표시합니다.

```
vdadmin -P -ld -xml -w
```

고유한 스타일시트 C:\Wtmp\Wunentitled-policies.xml을 적용하고 up-output.html 파일로 출력을 리디렉션합니다.

```
vdadmin -P -ld -xml -xsltpath "C:\Wtmp\Wunentitled-policies.xml" > up-output.html
```

-Q 옵션을 사용하여 키오스크 모드에서 클라이언트 구성

vdadmin 명령을 -Q 옵션과 함께 사용해 키오스크 모드에서 클라이언트 계정 생성 및 기본값 설정, 해당 클라이언트에 대한 인증 사용 설정, 그리고 클라이언트 구성 정보 표시 작업을 수행할 수 있습니다.

구문

```
vdadmin -Q -clientauth -add [-b authentication_arguments] -domain domain_name-clientid client_id [-password "password" | -genpassword] [-ou DN] [-expirepassword | -noexpirepassword] [-group group_name | -nogroup] [-description "description_text"]
```

```
vdadmin -Q -disable [-b authentication_arguments] -s connection_server
```

```
vdadmin -Q -enable [-b authentication_arguments] -s connection_server [-requirepassword]
```

```
vdadmin -Q -clientauth -getdefaults [-b authentication_arguments] [-xml]
```

```
vdadmin -Q -clientauth -list [-b authentication_arguments] [-xml]
```

```
vdadmin -Q -clientauth -remove [-b authentication_arguments] -domain domain_name-clientid client_id
```

```
vdadmin -Q -clientauth -removeall [-b authentication_arguments] [-force]
```

```
vdadmin -Q -clientauth -setdefaults [-b authentication_arguments] [-ou DN] [-expirepassword | -noexpirepassword] [-group group_name | -nogroup]
```

```
vdadmin -Q -clientauth -update [-b authentication_arguments] -domain domain_name-clientid client_id [-password "password" | -genpassword] [-description "description_text"]
```

사용 정보

클라이언트가 원격 데스크톱에 연결할 때 사용할 연결 서버 인스턴스가 포함된 그룹의 연결 서버 인스턴스 중 하나에서 vdadmin 명령을 실행해야 합니다.

암호 만료와 Active Directory 그룹 구성원에 대해 기본값을 구성하는 경우에는 그룹의 모든 연결 서버 인스턴스에서 이들 설정을 공유합니다.

키오스크 모드에서 클라이언트를 추가하는 경우 Horizon 7가 Active Directory에 클라이언트의 사용자 계정을 생성합니다. 클라이언트 이름을 지정할 경우 "Custom-" 또는 ADAM에서 정의할 수 있는 대체 문자열 중 하나로 시작하고 20자 미만이어야 합니다. 지정한 이름을 두 개 이상의 클라이언트 디바이스와 함께 사용해서는 안 됩니다.

연결 서버 인스턴스에서 ADAM의 cn=common,ou=global,ou=properties,dc=vdi,dc=vmware,dc=int 아래에 있는 pae-ClientAuthPrefix 다중 값 특성에 "custom-"에 대한 대체 접두사를 정의할 수 있습니다. 일반 사용자 계정에는 이러한 접두사를 사용하지 마십시오.

클라이언트 이름을 지정하지 않을 경우에는 클라이언트 디바이스용으로 지정된 MAC 주소를 사용해 Horizon 7에서 이름을 생성합니다. 예를 들어, MAC 주소가 00:10:db:ee:76:80인 경우 해당하는 계정 이름은 cm-00_10_db_ee_76_80입니다. 이러한 계정은 클라이언트를 인증할 수 있는 연결 서버 인스턴스에서만 사용할 수 있습니다.

일부 쉘 클라이언트는 "custom-" 또는 "cm-"으로 시작하는 계정 이름만 키오스크 모드에서 사용합니다.

암호는 16자로 자동 생성되며 대문자, 소문자, 기호, 숫자를 최소 하나 이상씩 포함하고 동일 문자를 반복 사용할 수 있습니다. 보안 수준이 높은 암호가 필요하다면 -password 옵션을 사용해 암호를 지정해야 합니다.

-group 옵션을 사용해 그룹을 지정하거나 이전에 기본 그룹을 설정한 경우에는 Horizon 7에서 이 그룹에 클라이언트 계정을 추가합니다. -nogroup 옵션을 지정해 임의의 그룹에 계정이 추가되지 않도록 방지할 수 있습니다.

키오스크 모드에서 클라이언트를 인증하도록 연결 서버 인스턴스를 설정하면 클라이언트에서 암호를 입력하도록 선택적으로 지정할 수 있습니다. 인증을 사용하지 않도록 설정하면 클라이언트가 원격 데스크톱에 연결할 수 없습니다.

개별 연결 서버 인스턴스에 대한 인증을 사용하거나 사용하지 않도록 설정해도 그룹에 있는 모든 연결 서버 인스턴스에서 클라이언트 인증에 대한 다른 설정을 모두 공유합니다. 클라이언트의 요청을 수락할 수 있도록 그룹의 모든 연결 서버 인스턴스에 대해 클라이언트를 한 번만 추가하면 됩니다.

인증을 사용하도록 설정할 때 -requirepassword 옵션을 지정하면 연결 서버 인스턴스에서는 암호가 자동 생성된 클라이언트를 인증할 수 없습니다. 연결 서버 인스턴스 구성을 변경해 이 옵션을 지정하면 이러한 클라이언트는 자신을 인증할 수 없어 인증이 실패하고 알 수 없는 사용자 이름 또는 잘못된 암호라는 오류 메시지가 표시됩니다.

옵션

다음 표에는 키오스크 모드에서 클라이언트 구성 시 지정할 수 있는 옵션이 나와 있습니다.

표 12-16. 키오스크 모드에서 클라이언트 구성 옵션

옵션	설명
-add	키오스크 모드에서 클라이언트 계정을 추가합니다.
-clientauth	키오스크 모드에서 클라이언트 인증을 구성하는 작업을 지정합니다.
-clientid client_id	클라이언트 이름 또는 MAC 주소를 지정합니다.

표 12-16. 키오스크 모드에서 클라이언트 구성 옵션 (계속)

옵션	설명
-description "description_text"	클라이언트 디바이스 계정에 대한 설명을 Active Directory에 생성합니다.
-disable	지정된 연결 서버 인스턴스에서 키오스크 모드로 클라이언트를 인증하지 않도록 설정합니다.
-domain domain_name	클라이언트 디바이스 계정의 도메인을 지정합니다.
-enable	지정된 연결 서버 인스턴스에서 키오스크 모드로 클라이언트를 인증하도록 설정합니다.
-expirepassword	클라이언트 계정의 암호 만료 시간을 연결 서버 그룹과 동일하게 지정합니다. 그룹의 암호 만료 시간을 정의하지 않은 경우에는 암호가 만료되지 않습니다.
-force	키오스크 모드에서 클라이언트 계정을 제거할 때 확인 메시지를 표시하지 않도록 설정합니다.
-genpassword	클라이언트 계정에 대한 암호를 생성합니다. -password 또는 -genpassword를 지정하지 않을 경우 기본으로 사용되는 동작입니다.
-getdefaults	클라이언트 계정 추가 시 사용하는 기본값을 가져옵니다.
-group group_name	클라이언트 계정을 추가할 기본 그룹의 이름을 지정합니다. 그룹의 이름은 Active Directory에서 Windows 2000 이전 그룹 이름으로 지정해야 합니다.
-list	키오스크 모드의 클라이언트 정보 및 키오스크 모드에서 클라이언트 인증을 사용하도록 설정한 연결 서버 인스턴스 정보를 표시합니다.
-noexpirepassword	계정 암호가 만료되지 않도록 지정합니다.
-nogroup	클라이언트 계정을 추가할 때 클라이언트 계정이 기본 그룹에 추가되지 않도록 지정합니다. 클라이언트의 기본값을 설정할 때 기본 그룹에 대한 설정을 지웁니다.
-ou DN	클라이언트 계정을 추가할 조직 단위의 고유 이름을 지정합니다. 예: OU=kiosk-ou,DC=myorg,DC=com 참고 -setdefaults 옵션을 사용해 조직 단위 구성을 변경할 수 없습니다.
-password "password"	클라이언트 계정에 대한 명시적 암호를 지정합니다.
-remove	키오스크 모드에서 클라이언트 계정을 제거합니다.
-removeall	키오스크 모드에서 모든 클라이언트 계정을 제거합니다.
-requirepassword	클라이언트가 키오스크 모드에서 암호를 입력하도록 지정합니다. Horizon 7에서 새 연결용으로 생성된 암호를 허용하지 않습니다.
-s connection_server	키오스크 모드에서 클라이언트 인증을 사용 또는 사용하지 않도록 설정할 연결 서버 인스턴스의 NetBIOS 이름을 지정합니다.

표 12-16. 키오스크 모드에서 클라이언트 구성 옵션 (계속)

옵션	설명
-setdefaults	클라이언트 계정 추가 시 사용하는 기본값을 설정합니다.
-update	키오스크 모드에서 클라이언트 계정을 업데이트합니다.

예제

클라이언트 그룹의 구성원, 암호 만료, 조직 단위에 대한 기본값을 설정하십시오.

```
vdadmin -Q -clientauth -setdefaults -ou "OU=kiosk-ou,DC=myorg,DC=com" -noexpirepassword -group kc-grp
```

현재 클라이언트의 기본값을 일반 텍스트 형식으로 가져옵니다.

```
vdadmin -Q -clientauth -getdefaults
```

현재 클라이언트의 기본값을 XML 형식으로 가져옵니다.

```
vdadmin -Q -clientauth -getdefaults -xml
```

그룹 kc-grp에 대한 기본 설정을 사용해서 MAC 주소로 지정된 클라이언트 계정을 MYORG 도메인에 추가합니다.

```
vdadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -group kc-grp
```

자동으로 생성된 암호를 사용해서 MAC 주소로 지정된 클라이언트 계정을 MYORG 도메인에 추가합니다.

```
vdadmin -Q -clientauth -add -domain MYORG -clientid 00:10:db:ee:76:80 -genpassword -ou "OU=kiosk-ou,DC=myorg,DC=com" -group kc-grp
```

명명된 클라이언트 계정을 추가하고 클라이언트에서 사용할 암호를 지정합니다.

```
vdadmin -Q -clientauth -add -domain MYORG -clientid custom-Terminal21 -password "guest" -ou "OU=kiosk-ou,DC=myorg,DC=com" -description "Terminal 21"
```

새 암호와 설명 텍스트를 지정해 클라이언트 계정을 업데이트합니다.

```
vdadmin -Q -clientauth -update -domain MYORG -clientid custom-Terminal21 -password "Secret1!" -description "Foyer Entry Workstation"
```

MAC 주소로 지정된 키오스크 클라이언트 계정을 MYORG 도메인에서 제거합니다.

```
vdadmin -Q -clientauth -remove -domain MYORG -clientid 00:10:db:ee:54:12
```


제거 확인 메시지를 표시하지 않고 모든 클라이언트 계정을 제거합니다.

```
vdadmin -Q -clientauth -removeall -force
```

연결 서버 인스턴스 csvr-2에 대한 클라이언트 인증을 사용하도록 설정합니다. 자동 생성된 암호를 갖는 클라이언트는 암호를 제공하지 않고 자신을 인증할 수 있습니다.

```
vdadmin -Q -enable -s csvr-2
```

연결 서버 인스턴스 csvr-3에 대한 클라이언트 인증을 사용하도록 설정하고 클라이언트가 Horizon Client에 대한 자신의 암호를 지정하도록 요구합니다. 암호가 자동 생성된 클라이언트는 자신을 인증할 수 없습니다.

```
vdadmin -Q -enable -s csvr-3 -requirepassword
```

연결 서버 인스턴스 csvr-1에 대한 클라이언트 계정을 사용하지 않도록 설정합니다.

```
vdadmin -Q -disable -s csvr-1
```

텍스트 형식으로 클라이언트에 대한 정보를 표시합니다. 클라이언트 cm-00_0c_29_0d_a3_e6의 암호는 자동으로 생성되었기 때문에 Horizon Client에 최종 사용자가 암호를 입력하거나 애플리케이션 스크립트를 통해 암호를 지정할 필요가 없습니다. 클라이언트 cm-00_22_19_12_6d_cf의 암호는 명시적으로 지정되었으며 최종 사용자가 이 암호를 입력해야 합니다. 연결 서버 인스턴스 CONSVR2는 암호가 자동 생성된 클라이언트의 인증 요청을 허용합니다. CONSVR1은 키오스크 모드에서 클라이언트의 인증 요청을 허용하지 않습니다.

```
C:\W vdadmin -Q -clientauth -list
Client Authentication User List
=====
GUID           : 94be6344-0c9b-4a92-8d54-1brc1c2dc282
ClientID       : cm-00_0c_29_0d_a3_e6
Domain        : myorg.com
Password Generated: true

GUID           : 471d9d35-68b2-40ee-b693-56a7d92b2e25
ClientID       : cm-00_22_19_12_6d_cf
Domain        : myorg.com
Password Generated: false

Client Authentication Connection Servers
=====
Common Name           : CONSVR1
Client Authentication Enabled : false
Password Required     : false

Common Name           : CONSVR2
Client Authentication Enabled : true
Password Required     : false
```

-R 옵션을 사용하여 시스템의 첫 번째 사용자 표시

vdmadmin 명령에 -R 옵션을 사용하여 관리되는 가상 시스템의 초기 할당을 확인할 수 있습니다. 예를 들어, LADP 데이터가 손실된 경우 사용자에게 가상 시스템을 다시 할당하려면 이 정보가 필요할 수 있습니다.

참고 -R 옵션을 사용한 vdmadmin 명령은 View Agent 5.1 이하 버전을 실행하는 가상 시스템에서만 작동합니다. View Agent 5.1 이상 및 Horizon Agent 7.0 이상 버전을 실행하는 가상 시스템에서는 이 옵션이 작동하지 않습니다. 가상 시스템의 첫 번째 사용자를 찾으려면 이벤트 데이터베이스를 사용하여 시스템에 로그인한 사용자를 확인하십시오.

구문

```
vdmadmin -R -i network_address
```

사용 정보

-b 옵션을 사용하면 권한 있는 사용자로 이 명령을 실행할 수 없습니다. **관리자** 역할의 사용자로 로그인해야 합니다.

옵션

-i 옵션은 가상 시스템의 IP 주소를 지정합니다.

예제

IP 주소가 10.20.34.120인 가상 시스템에 액세스한 첫 번째 사용자를 표시합니다.

```
vdmadmin -R -i 10.20.34.120
```

-S 옵션을 사용하여 연결 서버 인스턴스 또는 보안 서버의 항목 제거

vdmadmin 명령을 -S 옵션과 함께 사용하면 Horizon 7 구성에서 연결 서버 인스턴스 또는 보안 서버의 항목을 제거할 수 있습니다.

구문

```
vdmadmin -S [-b authentication_arguments] -r -s server
```

사용 정보

고가용성을 위해 Horizon 7에서는 연결 서버 그룹에 하나 이상의 연결 서버 인스턴스 복제본을 구성할 수 있습니다. 그룹에서 연결 서버 인스턴스를 사용하지 않도록 설정하면 서버에 대한 항목이 Horizon 7 구성 내에 보존됩니다.

vdmadmin 명령을 -S 옵션과 함께 사용하여 Horizon 7 환경에서 보안 서버를 제거할 수도 있습니다. 보안 서버를 영구적으로 제거하지 않고 업그레이드하거나 재설치하려는 경우 이 옵션을 사용할 필요가 없습니다.

영구적으로 제거할 경우 다음 작업을 수행하십시오.

- 1 연결 서버 설치 관리자를 실행하여 Windows Server 컴퓨터에서 연결 서버 인스턴스 또는 보안 서버를 제거합니다.
- 2 프로그램 추가 또는 제거 도구를 실행하여 Windows Server 컴퓨터에서 Adam 인스턴스 VMwareVDMDS 프로그램을 제거합니다.
- 3 다른 연결 서버 인스턴스에서 vdmadmin 명령을 사용하여 제거된 연결 서버 인스턴스 또는 보안 서버의 항목을 구성에서 제거합니다.

원래 그룹의 Horizon 7 구성을 복제하지 않고 제거한 시스템에 Horizon 7을 다시 설치하려는 경우에는 재설치를 수행하기 전에 원래 그룹에서 모든 연결 서버 호스트를 다시 시작해야 합니다. 이런 경우 다시 설치된 연결 서버 인스턴스가 원래의 그룹에서 구성 업데이트를 수신하지 않게 됩니다.

옵션

-s 옵션은 제거할 연결 서버 인스턴스 또는 보안 서버의 NetBIOS 이름을 지정합니다.

예제

연결 서버 인스턴스 connsvr3의 항목을 제거합니다.

```
vdmadmin -S -r -s connsvr3
```

-T 옵션을 사용하는 관리자에게 보조 자격 증명 제공

vdmadmin 명령을 -T 옵션과 함께 사용하여 관리자에게 Active Directory 보조 자격 증명을 제공할 수 있습니다.

구문

```
vdmadmin -T [-b authentication_arguments] -domainauth  
{-add | -update | -remove | -removeall | -list} -owner domain#user -user domain#user [-password password]
```

사용 정보

사용자와 그룹이 연결 서버 도메인과 한 방향으로 신뢰 관계에 있는 도메인에 있는 경우에는 Horizon Administrator에서 관리자에게 보조 자격 증명을 제공해야 합니다. 관리자는 이러한 사용자에게 신뢰할 수 있는 단방향 도메인에 대한 액세스 권한을 제공하려면 보조 자격 증명에 있어야 합니다. 신뢰할 수 있는 단방향 도메인은 외부 도메인이거나 전이적 포리스트 신뢰 관계에 있는 도메인일 수 있습니다.

보조 자격 증명은 최종 사용자의 데스크톱 또는 애플리케이션 세션이 아니라 Horizon Administrator 세션에만 필요합니다. 관리자 사용자만 보조 자격 증명에 필요합니다.

vdmadmin 명령을 사용하면 사용자별로 보조 자격 증명을 구성할 수 있습니다. 전역으로 지정된 보조 자격 증명을 구성할 수 없습니다.

포리스트 신뢰의 경우 일반적으로 포리스트 루트 도메인에 대해서만 보조 자격 증명을 구성할 수 있습니다. 그러면 연결 서버는 포리스트 신뢰 관계에 있는 하위 도메인을 열거할 수 있습니다.

Active Directory 계정 잠금, 사용 안 함 및 로그인 시간 확인은 신뢰할 수 있는 단방향 도메인에서 사용자가 처음으로 로그인할 때에만 수행할 수 있습니다.

신뢰할 수 있는 단방향 도메인에서는 사용자의 PowerShell 관리 및 스마트 카드 인증이 지원되지 않습니다. 신뢰할 수 있는 단방향 도메인에서의 사용자 SAML 인증은 지원되지 않습니다.

보조 자격 증명 계정에는 다음과 같은 사용 권한이 필요합니다. 표준 사용자 계정에는 이러한 사용 권한이 기본적으로 있어야 합니다.

- 목록 내용
- 모든 속성 읽기
- 사용 권한 읽기
- tokenGroupsGlobalAndUniversal 읽기(모든 속성 읽기에 내포)

제한 사항

- 신뢰할 수 있는 단방향 도메인의 사용자에게 대한 PowerShell 관리 및 스마트 카드 인증은 지원되지 않습니다.
- 신뢰할 수 있는 단방향 도메인에서의 사용자 SAML 인증은 지원되지 않습니다.

옵션

표 12-17. 보조 자격 증명 제공 옵션

옵션	설명
-add	소유자 계정에 보조 자격 증명을 추가합니다. 지정된 자격 증명에 유효한지 확인하기 위해 Windows 로그인 수행됩니다. View LDAP에서 사용자에게 대해 FSP(외부 보안 주체)가 생성됩니다.
-update	소유자 계정의 보조 자격 증명을 업데이트합니다. 업데이트 자격 증명에 유효한지 확인하기 위해 Windows 로그인 수행됩니다.
-list	소유자 계정의 보안 자격 증명을 표시합니다. 암호는 표시되지 않습니다.
-remove	소유자 계정의 보안 자격 증명 하나를 제거합니다.
-removeall	소유자 계정의 모든 보안 자격 증명을 제거합니다.

예제

지정된 소유자 계정에 보조 자격 증명을 추가합니다. 지정된 자격 증명에 유효한지 확인하기 위해 Windows 로그인이 수행됩니다.

```
vdadmin -T -domainauth -add -owner domain\User -user domain\User -password password
```

지정된 소유자 계정의 보조 자격 증명을 업데이트합니다. 업데이트 자격 증명에 유효한지 확인하기 위해 Windows 로그인이 수행됩니다.

```
vdadmin -T -domainauth -update -owner domain\User -user domain\User -password password
```

지정된 소유자 계정의 보조 자격 증명을 제거합니다.

```
vdadmin -T -domainauth -remove -owner domain\User -user domain\User
```

지정된 소유자 계정의 보조 자격 증명을 모두 제거합니다.

```
vdadmin -T -domainauth -removeall -owner domain\User
```

지정된 소유자 계정의 보조 자격 증명을 모두 표시합니다. 암호는 표시되지 않습니다.

```
vdadmin -T -domainauth -list -owner domain\User
```

-U 옵션을 사용한 사용자 정보 표시

vdadmin 명령을 -U 옵션과 함께 사용해 사용자 세부 정보를 표시할 수 있습니다.

구문

```
vdadmin -U [-b authentication_arguments] -u domain#user [-w | -n] [-xml]
```

사용 정보

이 명령은 Active Directory 및 Horizon 7에서 가져온 사용자 정보를 표시합니다.

- Active Directory에서 가져온 사용자 계정 세부 정보
- Active Directory 그룹 구성원 자격
- 시스템 ID, 디스플레이 이름, 설명, 폴더 및 시스템 사용 설정 여부를 포함한 시스템 권한
- ThinApp 할당
- 사용자의 관리 권한 및 관리 권한을 가진 폴더를 포함한 관리자 역할

옵션

-u 옵션은 사용자의 이름 및 도메인을 지정합니다.

예제

CORP 도메인에 있는 사용자 Jo에 대한 정보를 ASCII 문자를 사용해 XML 형식으로 표시하십시오.

```
vdadmin -U -u CORPWJo -n -xml
```

-V 옵션을 사용하여 가상 시스템 잠금 해제 또는 잠금

vdadmin 명령을 -V 옵션과 함께 사용하여 데이터 센터의 가상 시스템을 잠금 해제하거나 잠글 수 있습니다.

구문

```
vdadmin -V [-b authentication_arguments] -e -d desktop -m machine [-m machine] ...
```

```
vdadmin -V [-b authentication_arguments] -e -vcdn vCenter_dn -vmppath inventory_path
```

```
vdadmin -V [-b authentication_arguments] -p -d desktop -m machine [-m machine] ...
```

```
vdadmin -V [-b authentication_arguments] -p -vcdn vCenter_dn -vmppath inventory_path
```

사용 정보

원격 데스크톱이 잘못된 상태로 남게 되는 문제가 발생할 경우 가상 시스템의 잠금을 해제하거나 잠그는 용도로만 `vdmadmin` 명령을 사용해야 합니다. 이 명령을 사용하여 올바르게 작동하는 원격 데스크톱을 관리하지 마십시오.

원격 데스크톱이 잠기거나 가상 시스템의 항목이 ADAM에 더 이상 존재하지 않을 경우 `-vmPath` 및 `-vcdn` 옵션을 사용하여 가상 시스템 및 vCenter Server의 인벤토리 경로를 지정하십시오. vCenter Client를 사용하여 Home/Inventory/VMs and Templates 아래에서 원격 데스크톱의 가상 시스템 인벤토리 경로를 찾을 수 있습니다. ADAM ADSI Edit을 사용하여 OU=Properties 머리글 아래에서 vCenter Server의 고유 이름을 찾을 수 있습니다.

옵션

다음 표에는 가상 시스템을 잠금 해제하거나 잠그기 위해 지정할 수 있는 옵션이 나와 있습니다.

표 12-18. 가상 시스템의 잠금 해제 또는 잠금 옵션

옵션	설명
<code>-d desktop</code>	데스크톱 풀을 지정합니다.
<code>-e</code>	가상 시스템을 잠금 해제합니다.
<code>-m machine</code>	가상 시스템 이름을 지정합니다.
<code>-p</code>	가상 시스템을 잠급니다.
<code>-vcdn vCenter_dn</code>	vCenter Server의 고유 이름을 지정합니다.
<code>-vmPath inventory_path</code>	가상 시스템의 인벤토리 경로를 지정합니다.

예제

데스크톱 풀 `dtpool3`의 가상 시스템 `machine 1` 및 `machine2`를 잠금 해제합니다.

```
vdmadmin -V -e -d dtpool3 -m machine1 -m machine2
```

데스크톱 풀 `dtpool3`의 가상 시스템 `machine3`을 잠급니다.

```
vdmadmin -V -p -d dtpool3 -m machine3
```

-X 옵션을 사용한 LDAP 항목 및 스키마 충돌 감지 및 해결

`vdmadmin` 명령을 `-X` 옵션과 함께 사용하여 그룹의 복제된 연결 서버 인스턴스에서 LDAP 항목 충돌 및 LDAP 스키마 충돌을 감지하고 해결할 수 있습니다. 이 옵션을 사용하여 Cloud Pod 아키텍처 환경에서 LDAP 스키마 충돌을 감지하고 해결할 수도 있습니다.

구문

```
vdmadmin -X [-b authentication_arguments] -collisions [-resolve]
vdmadmin -X [-b authentication_arguments] -schemacollisions [-resolve] [-global]
```

사용 정보

둘 이상의 연결 서버 인스턴스에 중복된 LDAP 항목이 있으면 Horizon 7에서 LDAP 데이터의 무결성에 문제가 생길 수 있습니다. LDAP 복제를 사용할 수 없는 동안 업그레이드 작업을 수행하면 이러한 상태가 발생할 수 있습니다. Horizon 7에서 정기적으로 이러한 오류 조건을 확인하지만, 그룹 내의 연결 서버 인스턴스 중 하나에서 vdmadmin 명령을 실행하여 수동으로 LDAP 항목의 충돌을 감지하고 해결할 수도 있습니다.

LDAP 복제를 사용할 수 없는 동안 업그레이드 작업을 수행하면 LDAP 스키마 충돌도 발생할 수 있습니다. Horizon 7에서는 이러한 오류 조건을 확인하지 않으므로 vdmadmin 명령을 실행하여 LDAP 스키마 충돌을 수동으로 감지하고 해결해야 합니다.

옵션

다음 표에서는 LDAP 항목 충돌을 감지하고 해결하기 위해 지정할 수 있는 옵션을 보여 줍니다.

표 12-19. LDAP 항목 충돌 감지 및 해결 옵션

옵션	설명
-collisions	연결 서버 그룹에서 LDAP 항목 충돌을 감지하기 위한 작업을 지정합니다.
-resolve	LDAP 인스턴스에서 모든 LDAP 충돌을 해결합니다. 이 옵션을 지정하지 않으면 이 명령은 찾은 문제를 나열만 합니다.

다음 표에서는 LDAP 스키마 충돌을 감지하고 해결하기 위해 지정할 수 있는 옵션을 보여 줍니다.

표 12-20. LDAP 스키마 충돌 감지 및 해결 옵션

옵션	설명
-schemacollisions	연결 서버 그룹 또는 Cloud Pod 아키텍처 환경에서 LDAP 스키마 충돌을 감지하기 위한 작업을 지정합니다.
-resolve	LDAP 인스턴스에서 모든 LDAP 스키마 충돌을 해결합니다. 이 옵션을 지정하지 않으면 이 명령은 찾은 문제를 나열만 합니다.
-global	Cloud Pod 아키텍처 환경에서 전역 LDAP 인스턴스에 대해 검사 및 수정 작업을 적용합니다. 이 옵션을 지정하지 않으면 로컬 LDAP 인스턴스에 대해 검사가 실행됩니다.

예제

연결 서버 그룹에서 LDAP 항목 충돌을 감지합니다.

```
vdmadmin -X -collisions
```

로컬 LDAP 인스턴스에서 LDAP 항목 충돌을 감지하고 해결합니다.

```
vdmadmin -X -collisions -resolve
```

전역 LDAP 인스턴스에서 LDAP 스키마 충돌을 감지하고 해결합니다.

```
vdmadmin -X -schemacollisions -resolve -global
```