

# Windows Monitor — 정규 리포트

샘플IDC

IT 운영팀 | 2026년 05월 13일 15:10

1. 정보

2. 정책

3. 보안

4. 이력

7. WinRM

## 1. 서버 정보 / 리소스

▲ 제일 위로

# Windows Monitor — 1. 서버 정보 / 리소스

샘플IDC

IT 운영팀 | 2026년 05월 11일 13:39

18

전체 서버

1

연결 실패

3

디스크 경고

0

보안 이벤트

SMP-PC 10.0.20.50

테스트 서버

OS <b>Microsoft Windows Server 2012 R2 Standard</b>		버전 <b>6.3.9600</b>	도메인 <b>company.local</b>
CPU 현재 <b>2.5%</b>	MEM 현재 <b>35.8%</b>	마지막 부팅 <b>2025-11-22 16:03</b>	가동 일수 <b>169일</b>
제조사 <b>HP</b>	모델 <b>ProLiant DL360 G6</b>	CPU <b>Intel(R) Xeon(R) CPU L5520 @ 2.27GHz</b>	CPU 구성 <b>2 소켓 / 8 코어 / 16 논리</b>
RAM <b>96 GB</b>			

수집 시간: 2026-05-11 13:39

디스크

드라이브	레이블	전체	사용	여유	사용률
C:	System	101.4 GB	37.06 GB	64.34 GB	<b>36.5%</b>
H:	SSD-500GB-R1	476.94 GB	15.07 GB	461.87 GB	<b>3.2%</b>
I:	SSD-480GB-R1	447.1 GB	394.12 GB	52.98 GB	<b>88.2%</b>
K:	HDD-500GB-R1	498.05 GB	399.78 GB	98.27 GB	<b>80.3%</b>
L: <b>위험</b>	HDD-300GB-R1	332.03 GB	326.24 GB	5.79 GB	<b>98.3%</b>
M:	SSD-1TB-R0-NoBackup	953.84 GB	330.45 GB	623.39 GB	<b>34.6%</b>

Windows Backup

최근: 2026-05-10 00:00 **실패 (HR=2155348020)** 당일: 없음 (-)버전: 263원본: C: **36.5%** 37.06/101.4GB

I: **88.2%** 394.12/447.1GB H: **3.2%** 15.07/476.94GB K: **80.3%** 399.78/498.05GB

L: **98.3%** 326.24/332.03GB 저장소: **SMP-PC 2026\_03\_20 15:12 DISK\_01 29.7%** 2617.44/3725.85GB 여유

물리 디스크 / RAID **ssacli.exe**

**RAID 컨트롤러**

컨트롤러	상태	캐시	배터리
Smart Array P410i	<b>OK</b>	OK	

**물리 디스크 (7개)**

Bay 11:1:1 <b>1 TB</b> HDD <b>OK</b>	Bay 11:1:2 <b>1 TB</b> HDD <b>OK</b>	Bay 11:1:3 <b>512 GB</b> SSD <b>OK</b>	Bay 11:1:4 <b>512 GB</b> SSD <b>OK</b>	Bay 21:1:5 <b>480 GB</b> SSD <b>OK</b>	Bay 21:1:6 <b>480 GB</b> SSD <b>OK</b>	Bay 21:1:8 <b>1 TB</b> SSD <b>OK</b>
---	---	---	---	---	---	---

Hyper-V 게스트 VM 12대

VM 이름	상태	메모리 (사용/총용량)	CP U	가동 일수	VHD 사용량
DWKim(54)	Runni ng	5.9 GB	3%	1일	DWKim.vhdx: 97.63GB / 100GB (97.6%) <span>Dynamic</span>
admin-it02(53)	Runni ng	5.9 GB	2%	169일	admin-it02_0395637E-8BD9-475F-AF89-EC0F0692CA12.avhdx: 6.85GB / 100GB (6.8%) <span>Differencing</span>
admin-it01(51)	Runni ng	5.9 GB	4%	39일	admin-it01C_5B7583C5-5C08-43E6-A33F-6FC081B872C3.avhdx: 12.79GB / 100GB (12.8%) <span>Differencing</span> admin-it01D_8C32060E-6658-4BE8-A90A-62EBD3FA4062.avhdx: 0.04GB / 100GB (0%) <span>Differencing</span>
admin-it01-HA(62)	Runni ng	2.9 GB	0%	26일	admin-it01_haos_ova-17.2_FE15B709-C859-402D-AE78-7B5D1F8B2A7E.avhdx: 0.19GB / 32GB (0.6%) <span>Differencing</span>
KHW(60)	Runni ng	8 GB	0%	169일	KHW-C_5F3DA027-FA07-465B-AD23-2192520F3244.avhdx: 5.44GB / 100GB (5.4%) <span>Differencing</span> KHW-D_61040B12-F0F7-4BD3-8B9A-AFE8D753E9DE.avhdx: 0.04GB / 50GB (0.1%) <span>Differencing</span>
DEV_AP(121)	Off	0 GB	0%	0일	DEV_AP_C.vhdx: 95.72GB / 100GB (95.7%) <span>Dynamic</span> DEV_AP_D.vhdx: 14.63GB / 100GB (14.6%) <span>Dynamic</span>
DEV_SQL(120)	Off	0 GB	0%	0일	DEV_SQL_C.vhdx: 49.58GB / 100GB (49.6%) <span>Differencing</span> DEV_SQL_D.vhdx: 1.6GB / 100GB (1.6%) <span>Dynamic</span>
HanDong1	Off	0 GB	0%	0일	HanDong1-C_1C2939BC-0807-421C-8CC7-E03F43800A0C.avhdx: 0GB / 100GB (0%) <span>Differencing</span>
admin-it01-AI(61)	Off	0 GB	0%	0일	admin-it01-AI_88350021-FF26-4B9F-B13D-AEC46A805811.avhdx: 0GB / 100GB (0%) <span>Differencing</span>
SJLEE(52)	Off	0 GB	0%	0일	SJLEE_4AC3D46D-E8B2-4346-A7D2-8120375C30A0.avhdx: 0GB / 100GB (0%) <span>Differencing</span>
SunYouPC	Off	0 GB	0%	0일	PC100-0_DC9F74AF-D60F-4E80-AAE2-F5BA0185B7FE.avhdx: 0GB / 111.79GB (0%) <span>Differencing</span> PC100-1_DC9F74AF-D60F-4E80-AAE2-F5BA0185B7FE.avhdx: 0GB / 465.76GB (0%) <span>Differencing</span> PC100-2_DC9F74AF-D60F-4E80-AAE2-F5BA0185B7FE.avhdx: 0GB / 1.9GB (0%) <span>Differencing</span>
Win10ProBase_2G	Off	0 GB	0%	0일	Win10Pro.vhdx: 57GB / 100GB (57%) <span>Dynamic</span>

# VHOST-DR01 100.100.180.190

Hyper-V Host (DR) - 외부 점프서버

OS <b>Microsoft Windows Server 2012 R2 Standard</b>	버전 <b>6.3.9600</b>	도메인 <b>VMHOST.local</b>	
CPU 현재 <b>6.5%</b>	MEM 현재 <b>18.5%</b>	마지막 부팅 <b>2022-09-22 16:24</b>	가동 일수 <b>1326일</b>
제조사 <b>HP</b>	모델 <b>ProLiant DL380 G7</b>	CPU <b>Intel(R) Xeon(R) CPU X5650 @ 2.67GHz</b>	CPU 구성 <b>2 소켓 / 12 코어 / 24 논리</b>
RAM <b>108 GB</b>			

수집 시간: 2026-05-11 13:40


## 디스크

드라이브	레이블	전체	사용	여유	사용률
C:	System	194.97 GB	59.35 GB	135.62 GB	<div><div style="width: 30.4%;"></div></div> 30.4%
D: <b>경고</b>	Install	25.46 GB	23.48 GB	1.98 GB	<div><div style="width: 92.2%;"></div></div> 92.2%
L:	RAID5-6TB	6520.25 GB	5110.28 GB	1409.97 GB	<div><div style="width: 78.4%;"></div></div> 78.4%
X: <b>위험</b>	Backup	58.59 GB	57.44 GB	1.15 GB	<div><div style="width: 98%;"></div></div> 98%

## Windows Backup

최근: 2026-05-11 00:00 **성공** 당일: 00:00 (-)버전: 1947원본:  C: **30.4%** 59.35/194.97GB 저장소:

**Backup 98%** 1.15/58.59GB 여유

 물리 디스크 / RAID **ssacli.exe**

### RAID 컨트롤러

컨트롤러	상태	캐시	배터리
Smart Array P410	<b>OK</b>	OK	OK

### 물리 디스크 (8개)

Bay 11:1:1 1 TB HDD OK	Bay 11:1:2 1 TB HDD OK	Bay 11:1:3 1 TB HDD OK	Bay 11:1:4 1 TB HDD OK	Bay 21:1:5 1 TB HDD OK	Bay 21:1:6 1 TB HDD OK	Bay 21:1:7 1 TB HDD OK	Bay 21:1:8 1 TB HDD OK
---------------------------------	---------------------------------	---------------------------------	---------------------------------	---------------------------------	---------------------------------	---------------------------------	---------------------------------

VM 이름	상태	메모리 (사용/총용량)	CP U	가동 일 수	VHD 사용량
SMP-DC02(180.187)	Running	3.9 GB	0%	26일	SMP-DC02.vhdx: 25.13GB / 100GB (25.1%) <span>Dynamic</span>
SMP-EX02(180.180)	Off	0 GB	0%	0일	-
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제이상</p> </div> </div>					
SMP-SQL(11.250)	Off	0 GB	0%	0일	SMP-SQL-C.vhd: 100.14GB / 100GB (100.1%) <span>Dynamic</span> SMP-SQL-D.vhd: 2.3GB / 100GB (2.3%) <span>Dynamic</span> SMP-SQL-E.vhd: 0.85GB / 300GB (0.3%) <span>Dynamic</span> SMP-SQL-L.vhd: 1.43GB / 200GB (0.7%) <span>Dynamic</span> SMP-SQL-S.vhdx: 12.5GB / 100GB (12.5%) <span>Dynamic</span>
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제정상</p> </div> </div>					
SAMPLEIDC-SMTP	Off	0 GB	0%	0일	SAMPLEIDC-SMTP.vhdx: 99.66GB / 100GB (99.7%) <span>Dynamic</span> SAMPLEIDC-Smtp-D.vhdx: 2.1GB / 100GB (2.1%) <span>Dynamic</span>
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제정상</p> </div> </div>					
SMP-WEB	Off	0 GB	0%	0일	SMP-WEB.vhd: 92.06GB / 127GB (72.5%) <span>Dynamic</span> SMP-WEB-D.vhd: 15.88GB / 200GB (7.9%) <span>Dynamic</span>
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제정상</p> </div> </div>					
CORP-LG-API(227.196)	Off	0 GB	0%	0일	API-C.vhdx: 50.88GB / 200GB (25.4%) <span>Dynamic</span> API-D.vhdx: 109.25GB / 200GB (54.6%) <span>Dynamic</span>
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제정상</p> </div> </div>					
CORP-LG-IM	Off	0 GB	0%	0일	IM-C.vhdx: 31.41GB / 200GB (15.7%) <span>Dynamic</span> IM-D.vhdx: 4.57GB / 200GB (2.3%) <span>Dynamic</span>
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제정상</p> </div> </div>					
CORP-LG-SSO	Off	0 GB	0%	0일	SSO-C.vhdx: 49.38GB / 200GB (24.7%) <span>Dynamic</span> SSO-D.vhdx: 32.44GB / 200GB (16.2%) <span>Dynamic</span>
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제정상</p> </div> </div>					
samplepro	Off	0 GB	0%	0일	samplepro.vhdx: 76.66GB / 100GB (76.7%) <span>Dynamic</span>
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제정상</p> </div> </div>					
Remote21	Off	0 GB	0%	0일	Remote21.vhdx: 44.91GB / 100GB (44.9%) <span>Dynamic</span>
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제정상</p> </div> </div>					
REMOTE-A	Off	0 GB	0%	0일	REMOTE-A.vhdx: 51.57GB / 100GB (51.6%) <span>Dynamic</span>
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제정상</p> </div> </div>					
REMOTE-B	Off	0 GB	0%	0일	REMOTE-B.vhdx: 52.6GB / 100GB (52.6%) <span>Dynamic</span>
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제정상</p> </div> </div>					
REMOTE-C	Off	0 GB	0%	0일	REMOTE-C.vhdx: 74.35GB / 100GB (74.4%) <span>Dynamic</span>
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제정상</p> </div> </div>					
Test01(180.181)	Off	0 GB	0%	0일	Win2012R2-Test01.vhdx: 18.72GB / 100GB (18.7%) <span>Dynamic</span>
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제정상</p> </div> </div>					
CORP1-APP(227.204)	Off	0 GB	0%	0일	CORP1-APP.vhdx: 99.85GB / 100GB (99.8%) <span>Dynamic</span> CORP1-APP-D.vhd: 21.48GB / 100GB (21.5%) <span>Dynamic</span>
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제정상</p> </div> </div>					
CORP1-MAIL	Off	0 GB	0%	0일	CORP1-MAIL.vhdx: 119.72GB / 120GB (99.8%) <span>Dynamic</span> CORP1-MAIL-D.vhdx: 192.07GB / 200GB (96%) <span>Dynamic</span>
<div style="display: flex; justify-content: space-between; align-items: center;"> <div> <p>복제본</p> <p>복제정상</p> </div> </div>					

VM 이름	상태	메모리 (사용/총용량)	CP U	가동 일수	VHD 사용량
samplepro-Win2016	Off	0 GB	0%	0일	 <span>Dynamic</span> <span>Dynamic</span>
Test233(이과장233)	Off	0 GB	0%	0일	<span>Dynamic</span> <span>Dynamic</span>
Win10Pro_base	Off	0 GB	0%	0일	<span>Dynamic</span>
Win2012R2G2-Base	Off	0 GB	0%	0일	<span>Dynamic</span>
Win2019-Base	Off	0 GB	0%	0일	<span>Dynamic</span>
Win2022-Base	Off	0 GB	0%	0일	<span>Dynamic</span>

## SMP-DC02 (샘플IDC) 100.100.180.187

Hyper-V Guest (SAMPLECORP 도메인)

OS <b>Microsoft Windows Server 2022 Standard</b>		버전 <b>10.0.20348</b>	도메인 <b>samplecorp.local</b>
CPU 현재 <b>5%</b>	MEM 현재 <b>63.4%</b>	마지막 부팅 <b>2026-04-15 15:34</b>	가동 일수 <b>25일</b>
제조사 <b>Microsoft Corporation</b>	모델 <b>Virtual Machine</b>	CPU <b>Intel(R) Xeon(R) CPU X5650 @ 2.67GHz</b>	
CPU 구성 <b>1 소켓 / 4 코어 / 4 논리</b>	RAM <b>3.9 GB</b>		

수집 시간: 2026-05-11 13:42

### 디스크

드라이브	레이블	전체	사용	여유	사용률
C:		99.32 GB	22.56 GB	76.76 GB	<b>22.7%</b>

# CORP1-MAIL (샘플IDC) 200.200.227.205

Hyper-V Guest (CORP1)

OS <b>Microsoft Windows Server 2012 R2 Standard</b>	버전 <b>6.3.9600</b>	도메인 <b>Workgroup: CORP1</b>	
CPU 현재 <b>1%</b>	MEM 현재 <b>45.9%</b>	마지막 부팅 <b>2026-04-21 12:03</b>	가동 일수 <b>20일</b>
제조사 <b>Microsoft Corporation</b>	모델 <b>Virtual Machine</b>	CPU <b>Intel(R) Xeon(R) CPU E5530 @ 2.40GHz</b>	
CPU 구성 <b>1 소켓 / 4 코어 / 4 논리</b>	RAM <b>4.9 GB</b>		

수집 시간: 2026-05-11 13:48

## 디스크

드라이브	레이블	전체	사용	여유	사용률
C:	CORP1-MAIL2	119.66 GB	103.88 GB	15.78 GB	86.8%
D:	MailData	139.06 GB	116.42 GB	22.64 GB	83.7%

## Windows Backup

최근: 2019-06-12 22:00 **실패 (HR=2155348061)** 당일: 없음 (-)버전: 22원본:

C: **86.8%** 103.88/119.66GB 저장소: **Etc 0%** 0/0GB 여유

기타사항: 워크그룹 CORP1 / 로컬계정 .Wvadmin

# VHOST-01 10.0.10.11

Hyper-V Host (IDC 내부)

OS <b>Microsoft Windows Server 2012 R2 Standard</b>	버전 <b>6.3.9600</b>	도메인 <b>VMHOST.local</b>	
CPU 현재 <b>1.5%</b>	MEM 현재 <b>68.5%</b>	마지막 부팅 <b>2026-04-20 08:34</b>	가동 일수 <b>21일</b>
제조사 <b>HP</b>	모델 <b>ProLiant DL360 G6</b>	CPU <b>Intel(R) Xeon(R) CPU X5650 @ 2.67GHz</b>	CPU 구성 <b>2 소켓 / 12 코어 / 12 논리</b>
RAM <b>64 GB</b>			

수집 시간: 2026-05-11 13:42

## 디스크


드라이브	레이블	전체	사용	여유	사용률
C:	System	136.35 GB	86.21 GB	50.14 GB	<b>63.2%</b>
I:	SSD-1TB	931.48 GB	358.63 GB	572.85 GB	<b>38.5%</b>
K:	HDD1TB	930 GB	63.9 GB	866.1 GB	<b>6.9%</b>

## Windows Backup

최근: 2026-05-11 00:00 **성공** 당일: 00:00 (-)버전: 1608원본:  K: **6.9%** 63.9/930GB

I: **38.5%** 358.63/931.48GB C: **63.2%** 86.21/136.35GB **저장소:**

**VHOST-01 2024\_08\_26 15:30 DISK\_01 89.8%** 285.24/2794.34GB 여유

 **ssacli.exe**

### RAID 컨트롤러

컨트롤러	상태	캐시	배터리
Smart Array P410i	<b>OK</b>	OK	Failed

### 물리 디스크 (6개)

Bay 11:1:1 <b>146 GB</b> HDD OK	Bay 11:1:2 <b>146 GB</b> HDD OK	Bay 21:1:5 <b>1 TB</b> HDD OK	Bay 21:1:6 <b>1 TB</b> HDD OK	Bay 21:1:7 <b>1 TB</b> SSD OK	Bay 21:1:8 <b>1 TB</b> SSD OK
--	--	--	--	--	--

Hyper-V 게스트 VM 3대

VM 이름	상태	메모리 (사용/총용량)	CP U	가동 일수	VHD 사용량
CORP-LG-API(227.196)	Running	20.5 GB	0%	20일	API-C.vhdx: 48.69GB / 200GB (24.3%) <span>Dynamic</span> API-D.vhdx: 109.19GB / 200GB (54.6%) <span>Dynamic</span>
<span>원본</span> <span>복제정상</span>					
CORP-LG-SSO(227.195)	Running	11.7 GB	0%	20일	SSO-C_5C05DFC2-479C-439F-8111-F6488C46CD08.avhdx: 14.51GB / 200GB (7.3%) <span>Differencing</span> SSO-D_557F2CAF-DADF-41C6-BDB0-9994A1A8E468.avhdx: 16.68GB / 200GB (8.3%) <span>Differencing</span>
<span>원본</span> <span>복제정상</span>					
CORP1-APP(227.204)	Running	8 GB	8%	20일	CORP1-APP.vhdx: 95.63GB / 100GB (95.6%) <span>Dynamic</span> CORP1-APP-D.vhd: 21.48GB / 100GB (21.5%) <span>Dynamic</span>
<span>원본</span> <span>복제정상</span>					

CORP1-APP (샘플IDC) 200.200.227.204

Hyper-V Guest (CORP1)

OS <b>Microsoft Windows Server 2012 R2 Standard</b>		버전 <b>6.3.9600</b>	도메인 <b>Workgroup: CORP1</b>
CPU 현재 <b>1%</b>	MEM 현재 <b>42%</b>	마지막 부팅 <b>2026-04-20 08:38</b>	가동 일수 <b>21일</b>
제조사 <b>Microsoft Corporation</b>	모델 <b>Virtual Machine</b>	CPU <b>Intel(R) Xeon(R) CPU X5650 @ 2.67GHz</b>	
CPU 구성 <b>1 소켓 / 6 코어 / 6 논리</b>	RAM <b>8 GB</b>		

수집 시간: 2026-05-11 13:48

디스크

드라이브	레이블	전체	사용	여유	사용률
C:	Duzon	99.66 GB	69.6 GB	30.06 GB	<b>69.8%</b>
D:	Etc	100 GB	19.77 GB	80.23 GB	<b>19.8%</b>

Windows Backup

최근: 2019-09-07 23:00 실패 (HR=2155348061) 당일: 없음 (-)버전: 118원본: D: **19.8%** 19.77/100GB

C: **69.8%** 69.6/99.66GB 저장소: CORP1-D 2016\_12\_30 23:42 DISK\_02 **0%** 0/0GB 여유

CORP1-D 2017\_07\_31 16:50 DISK\_02 **0%** 0/0GB 여유

기타사항: 워크그룹 CORP1 / 로컬계정 .\vmadmin

# VHOST-03 10.0.10.13

Hyper-V Host (IDC 내부)

OS <b>Microsoft Windows Server 2012 R2 Standard</b>	버전 <b>6.3.9600</b>	도메인 <b>VMHOST.local</b>	
CPU 현재 <b>8%</b>	MEM 현재 <b>71.6%</b>	마지막 부팅 <b>2022-09-06 11:10</b>	가동 일수 <b>1343일</b>
제조사 <b>HP</b>	모델 <b>ProLiant DL360 G6</b>	CPU <b>Intel(R) Xeon(R) CPU E5530 @ 2.40GHz</b>	CPU 구성 <b>1 소켓 / 4 코어 / 8 논리</b>
RAM <b>48 GB</b>			

수집 시간: 2026-05-11 13:42

## 디스크

드라이브	레이블	전체	사용	여유	사용률
C:	System	97.63 GB	40.81 GB	56.82 GB	<b>41.8%</b>
J:	BAY34-SSD450	446.78 GB	287 GB	159.78 GB	<b>64.2%</b>
K:	BAY56-SATA1TB	931.48 GB	512.7 GB	418.78 GB	<b>55%</b>

## Windows Backup

최근: 2026-05-11 00:00 **성공** 당일: 00:00 (-)버전: 476원본: C: **41.8%** 40.81/97.63GB

K: **55%** 512.7/931.48GB J: **64.2%** 287/446.78GB **저장소:**

**VHOST-03 2024\_10\_24 16:43 DISK\_01 83.5%** 459.82/2794.34GB 여유

물리 디스크 / RAID **ssacli.exe**

### RAID 컨트롤러

컨트롤러	상태	캐시	배터리
Smart Array P410i	<b>OK</b>	OK	

### 물리 디스크 (6개)

Bay 11:1:1 <b>146 GB</b> HDD OK	Bay 11:1:2 <b>146 GB</b> HDD OK	Bay 11:1:3 <b>480 GB</b> SSD OK	Bay 11:1:4 <b>480 GB</b> SSD OK	Bay 21:1:5 <b>1 TB</b> HDD OK	Bay 21:1:6 <b>1 TB</b> HDD OK
--	--	--	--	--	--

Hyper-V 게스트 VM 6대

VM 이름	상태	메모리 (사용/총용량)	CP U	가동 일 수	VHD 사용량
SMP-SQL(11.250) <span>원본</span> <span>복제정상</span>	Runnin g	7.8 GB	0%	425일	SMP-SQL-C.vhd: 100.14GB / 100GB (100.1%) <span>Dynamic</span> SMP-SQL-D.vhd: 2.3GB / 100GB (2.3%) <span>Dynamic</span> SMP-SQL-E.vhd: 0.85GB / 300GB (0.3%) <span>Dynamic</span> SMP-SQL-L.vhd: 1.43GB / 200GB (0.7%) <span>Dynamic</span> SMP-SQL-S.vhdx: 12.5GB / 100GB (12.5%) <span>Dynamic</span>
SMP-WEB(180.184) <span>원본</span> <span>복제정상</span>	Runnin g	2.9 GB	0%	681일	SMP-WEB.vhd: 92.19GB / 127GB (72.6%) <span>Dynamic</span> SMP-WEB-D.vhd: 15.9GB / 200GB (8%) <span>Dynamic</span> SMP-WEB-Y.vhd: 100.16GB / 100GB (100.2%) <span>Dynamic</span>
samplepro-Web(227.194) <span>원본</span> <span>복제정상</span>	Runnin g	8 GB	0%	681일	samplepro.vhdx: 58.29GB / 100GB (58.3%) <span>Dynamic</span>
REMOTE-A <span>원본</span> <span>복제정상</span>	Runnin g	4 GB	0%	145일	REMOTE-A.vhdx: 47.22GB / 100GB (47.2%) <span>Dynamic</span>
CORP1-MAIL(227.205) <span>원본</span> <span>복제정상</span>	Runnin g	4.9 GB	1%	18일	CORP1-MAIL.vhdx: 106.54GB / 120GB (88.8%) <span>Dynamic</span> CORP1-MAIL-D.vhdx: 188.6GB / 200GB (94.3%) <span>Dynamic</span>
Remote샘플대(180.189) <span>원본</span> <span>복제정상</span>	Off	0 GB	0%	0일	Remote21.vhdx: 36.82GB / 100GB (36.8%) <span>Dynamic</span>

## SMP-SQL (샘플IDC) 10.0.30.250

Hyper-V Guest (내부)

OS <b>Microsoft Windows Server 2008 R2 Standard</b>	버전 <b>6.1.7601</b>	도메인 <b>Workgroup: SAMPLEIDC</b>	
CPU 현재 <b>2%</b>	MEM 현재 <b>74.4%</b>	마지막 부팅 <b>2024-11-18 13:41</b>	가동 일수 <b>539일</b>
제조사 <b>Microsoft Corporation</b>	모델 <b>Virtual Machine</b>	CPU <b>Intel(R) Xeon(R) CPU E5530 @ 2.40GHz</b>	
CPU 구성 <b>1 소켓 / 6 코어 / 6 논리</b>	RAM <b>7.8 GB</b>		

수집 시간: 2026-05-11 13:45

### 디스크

드라이브	레이블	전체	사용	여유	사용률
C:	System	99.9 GB	86.47 GB	13.43 GB	<b>86.6%</b>
D:	SqlApp	100 GB	2.25 GB	97.75 GB	<b>2.2%</b>
E:	SqlData	300 GB	0.65 GB	299.35 GB	<b>0.2%</b>
L:	SqlLog	100 GB	0.52 GB	99.48 GB	<b>0.5%</b>
M:	SqlTemp	100 GB	1.06 GB	98.94 GB	<b>1.1%</b>
S:	Install	100 GB	7.58 GB	92.42 GB	<b>7.6%</b>

## REMOTE-A (샘플IDC) 10.0.30.55

샘플IDC 원격접속 서버

OS <b>Microsoft Windows 10 Pro</b>	버전 <b>10.0.19045</b>	도메인 <b>Workgroup: WORKGROUP</b>	CPU 현재 <b>1%</b>
MEM 현재 <b>75.2%</b>	마지막 부팅 <b>2025-11-18 17:42</b>	가동 일수 <b>173일</b>	
제조사 <b>Microsoft Corporation</b>	모델 <b>Virtual Machine</b>	CPU <b>Intel(R) Xeon(R) CPU E5530 @ 2.40GHz</b>	
CPU 구성 <b>1 소켓 / 6 코어 / 6 논리</b>	RAM <b>4 GB</b>		

수집 시간: 2026-05-11 13:49

### 디스크

드라이브	레이블	전체	사용	여유	사용률
C:		98.89 GB	34.48 GB	64.41 GB	<b>34.9%</b>

기타사항: 워크그룹 WORKGROUP / 로컬계정 .\remote

# VHOST-31 10.0.10.31

Hyper-V Host (IDC 내부)

OS <b>Microsoft Windows Server 2012 R2 Standard</b>	버전 <b>6.3.9600</b>	도메인 <b>VMHOST.local</b>	
CPU 현재 <b>1%</b>	MEM 현재 <b>57.4%</b>	마지막 부팅 <b>2026-05-01 15:24</b>	가동 일수 <b>9일</b>
제조사 <b>HP</b>	모델 <b>ProLiant DL380 G7</b>	CPU <b>Intel(R) Xeon(R) CPU X5660 @ 2.80GHz</b>	CPU 구성 <b>2 소켓 / 12 코어 / 12 논리</b>
RAM <b>72 GB</b>			

수집 시간: 2026-05-11 13:43

## 디스크

드라이브	레이블	전체	사용	여유	사용률
C:	SYSTEM	97.31 GB	40.83 GB	56.48 GB	42%
D:	Temp	181.71 GB	76.8 GB	104.91 GB	42.3%
I:	SSD-1TB	953.84 GB	556.25 GB	397.59 GB	58.3%
J:	SSD-450GB-NoBackup	440 GB	139.92 GB	300.08 GB	31.8%
K:	SAS-1TB-650GB	652.11 GB	125.08 GB	527.03 GB	19.2%

## Windows Backup

최근: 2026-05-11 00:00 **성공** 당일: 00:00 (-)버전: 1244원본:  K: **19.2%** 125.08/652.11GB

I: **58.3%** 556.25/953.84GB C: **42%** 40.83/97.31GB **저장소:**

VHOST-31 2024\_08\_27 16:57 DISK\_01 **44.1%** 1042.25/1862.87GB 여유

## 물리 디스크 / RAID **ssacli.exe**

컨트롤러	상태	캐시	배터리
Smart Array P410i	<b>OK</b>	OK	

## 물리 디스크 (6개 / 장애 1)

Bay 11:1:1 <b>1 TB</b> HDD OK	Bay 11:1:2 <b>1 TB</b> HDD OK	Bay 11:1:3 <b>480 GB</b> SSD OK	Bay 11:1:4 <b>480 GB</b> SSD OK	Bay 21:1:5 <b>1 TB</b> SSD <b>Predictive Failure</b>	Bay 21:1:6 <b>1 TB</b> SSD OK
--	--	--	--	---	--

Hyper-V 게스트 VM 5대

VM 이름	상태	메모리 (사용/총용량)	CP U	가동 일수	VHD 사용량
SMP-EX02(180.180)	Runn g	20 GB	0%	1일	SMP-EX02.vhdx: 250.29GB / 500GB (50.1%) <span>Dynamic</span> SMP-EX02_D.vhd: 249.79GB / 900GB (27.8%) <span>Dynamic</span>
SMP-SMTP(227.226)	Runn g <span>원본</span> <span>복제정상</span>	4 GB	0%	9일	SAMPLEIDC-SMTP.vhdx: 68.38GB / 100GB (68.4%) <span>Dynamic</span> SAMPLEIDC-Smtp-D.vhd: 2.1GB / 100GB (2.1%) <span>Dynamic</span>
SMP-WEB	Runn g	5.9 GB	0%	1일	SMP-WEB.vhdx: 25.32GB / 100GB (25.3%) <span>Dynamic</span> SMP-WEB-D.vhd: 8.16GB / 100GB (8.2%) <span>Dynamic</span>
REMOTE-B	Runn g <span>원본</span> <span>복제정상</span>	4 GB	0%	10일	REMOTE-B.vhdx: 49.47GB / 100GB (49.5%) <span>Dynamic</span>
REMOTE-C	Runn g <span>원본</span> <span>복제정상</span>	4 GB	8%	10일	REMOTE-C.vhdx: 71.07GB / 100GB (71.1%) <span>Dynamic</span>

SMP-WEB (샘플IDC) 100.100.180.184

Hyper-V Guest

OS <b>Microsoft Windows Server 2022 Standard</b>		버전 <b>10.0.20348</b>	도메인 <b>Workgroup: SAMPLEIDC</b>
CPU 현재 <b>7%</b>	MEM 현재 <b>47.7%</b>	마지막 부팅 <b>2026-05-07 14:58</b>	가동 일수 <b>4일</b>
제조사 <b>Microsoft Corporation</b>	모델 <b>Virtual Machine</b>	CPU <b>Intel(R) Xeon(R) CPU X5660 @ 2.80GHz</b>	
CPU 구성 <b>1 소켓 / 4 코어 / 4 논리</b>	RAM <b>5.9 GB</b>		

수집 시간: 2026-05-11 13:46

디스크

드라이브	레이블	전체	사용	여유	사용률
C:		99.32 GB	23.63 GB	75.69 GB	<b>23.8%</b>
D:	DATA	100 GB	8.1 GB	91.9 GB	<b>8.1%</b>



# SMP-EX02 (샘플IDC) 100.100.180.180

Hyper-V Guest (mailhost)

OS <b>Microsoft Windows Server 2008 R2 Standard</b>	버전 <b>6.1.7601</b>	도메인 <b>samplemail.local</b>	
CPU 현재 <b>4%</b>	MEM 현재 <b>84.8%</b>	마지막 부팅 <b>2026-05-01 15:27</b>	가동 일수 <b>9일</b>
제조사 <b>Microsoft Corporation</b>	모델 <b>Virtual Machine</b>	CPU <b>Intel(R) Xeon(R) CPU X5660 @ 2.80GHz</b>	
CPU 구성 <b>1 소켓 / 6 코어 / 6 논리</b>	RAM <b>20 GB</b>		

수집 시간: 2026-05-11 13:46

## 디스크

드라이브	레이블	전체	사용	여유	사용률
C:	SMP-EX02	248.73 GB	71.87 GB	176.86 GB	 28.9%
D:	Exchange	347.65 GB	227.91 GB	119.74 GB	 65.6%

## Windows Backup

최근: - **성공** 당일: 없음 (-)버전: 0원본: 미설정저장소: 미설정

## SMP-SMTP (샘플IDC) 200.200.227.226

Hyper-V Guest

OS <b>Microsoft Windows Server 2012 R2 Standard</b>	버전 <b>6.3.9600</b>	도메인 <b>Workgroup: SAMPLEIDC</b>	
CPU 현재 <b>1%</b>	MEM 현재 <b>17.4%</b>	마지막 부팅 <b>2026-05-01 15:26</b>	가동 일수 <b>9일</b>
제조사 <b>Microsoft Corporation</b>	모델 <b>Virtual Machine</b>	CPU <b>Intel(R) Xeon(R) CPU X5660 @ 2.80GHz</b>	
CPU 구성 <b>1 소켓 / 6 코어 / 6 논리</b>	RAM <b>4 GB</b>		

수집 시간: 2026-05-11 13:47

### 디스크

드라이브	레이블	전체	사용	여유	사용률
C:	System	99.48 GB	67.69 GB	31.79 GB	<div style="width: 68%;"></div> 68%
D:	Install	100 GB	2 GB	98 GB	<div style="width: 2%;"></div> 2%

### Windows Backup

최근: - **성공** 당일: 없음 (-)버전: 0원본: 미설정저장소: 미설정

## REMOTE-B (샘플IDC) 10.0.30.56

샘플IDC 원격접속 서버

OS <b>Microsoft Windows 10 Pro</b>	버전 <b>10.0.19045</b>	도메인 <b>Workgroup: WORKGROUP</b>	CPU 현재 <b>0%</b>
MEM 현재 <b>76%</b>	마지막 부팅 <b>2026-05-01 15:26</b>	가동 일수 <b>9일</b>	
제조사 <b>Microsoft Corporation</b>	모델 <b>Virtual Machine</b>	CPU <b>Intel(R) Xeon(R) CPU X5660 @ 2.80GHz</b>	
CPU 구성 <b>1 소켓 / 6 코어 / 6 논리</b>	RAM <b>4 GB</b>		

수집 시간: 2026-05-11 13:49

### 디스크

드라이브	레이블	전체	사용	여유	사용률
C:		98.89 GB	33.86 GB	65.03 GB	<div style="width: 34.2%;"></div> 34.2%

기타사항: 워크그룹 WORKGROUP / 로컬계정 .\remote

# REMOTE-C (샘플IDC) 10.0.30.57

샘플IDC 원격접속 서버

OS <b>Microsoft Windows 10 Pro</b>	버전 <b>10.0.19045</b>	도메인 <b>Workgroup: WORKGROUP</b>	CPU 현재 <b>1%</b>
MEM 현재 <b>71.1%</b>	마지막 부팅 <b>2026-05-01 15:26</b>	가동 일수 <b>9일</b>	
제조사 <b>Microsoft Corporation</b>	모델 <b>Virtual Machine</b>	CPU <b>Intel(R) Xeon(R) CPU X5660 @ 2.80GHz</b>	
CPU 구성 <b>1 소켓 / 6 코어 / 6 논리</b>	RAM <b>4 GB</b>		

수집 시간: 2026-05-11 13:49

## 디스크

드라이브	레이블	전체	사용	여유	사용률
C:		98.89 GB	44.76 GB	54.13 GB	<b>45.3%</b>

기타사항: 워크그룹 WORKGROUP / 로컬계정 .#remote

# VHOST-32 10.0.10.32

Hyper-V Host (IDC 내부)

OS <b>Microsoft Windows Server 2012 R2 Standard</b>	버전 <b>6.3.9600</b>	도메인 <b>VMHOST.local</b>	
CPU 현재 <b>4%</b>	MEM 현재 <b>19.6%</b>	마지막 부팅 <b>2024-07-03 16:22</b>	가동 일수 <b>676일</b>
제조사 <b>HP</b>	모델 <b>ProLiant DL380 G6</b>	CPU <b>Intel(R) Xeon(R) CPU X5650 @ 2.67GHz</b>	CPU 구성 <b>2 소켓 / 12 코어 / 12 논리</b>
RAM <b>96 GB</b>			

수집 시간: 2026-05-11 13:44

## 디스크

드라이브	레이블	전체	사용	여유	사용률
C:	System	97.63 GB	51.6 GB	46.03 GB	52.9%
D:	Temp	39.06 GB	1.39 GB	37.67 GB	3.6%
I:	SSD-450GB	447.1 GB	249.95 GB	197.15 GB	55.9%
J:	SSD-480GB	447.1 GB	107.22 GB	339.88 GB	24%
K:	HDD-1TB	930 GB	263.62 GB	666.38 GB	28.3%

## Windows Backup

최근: 2026-05-10 21:00 **성공** 당일: 없음 (-) 버전: 1064 원본: C: **52.9%** 51.6/97.63GB  
J: **24%** 107.22/447.1GB K: **28.3%** 263.62/930GB I: **55.9%** 249.95/447.1GB 저장소:  
VHOST-32 2025\_09\_08 23:07 DISK\_01 **93.3%** 188.48/2794.34GB 여유

## 물리 디스크 / RAID **ssacli.exe**

### RAID 컨트롤러

컨트롤러	상태	캐시	배터리
Smart Array P410i	<b>OK</b>	OK	OK

### 물리 디스크 (8개)

Bay 11:1:1 <b>146 GB</b> HDD OK	Bay 11:1:2 <b>146 GB</b> HDD OK	Bay 11:1:3 <b>1 TB</b> HDD OK	Bay 11:1:4 <b>1 TB</b> HDD OK	Bay 21:1:5 <b>480 GB</b> SSD OK	Bay 21:1:6 <b>480 GB</b> SSD OK	Bay 21:1:7 <b>480 GB</b> SSD OK	Bay 21:1:8 <b>480 GB</b> SSD OK
--	--	--	--	--	--	--	--

Hyper-V 게스트 VM 3대

VM 이름	상태	메모리 (사용/총용량)	CP U	가동 일 수	VHD 사용량
SMP-DC01(180.182)	Runnin g	3.9 GB	0%	1일	SMP-DC01.vhdx: 25GB / 100GB (25%) <span>Dynamic</span>
CORP-LG-IM(197)	Runnin g	5.9 GB	0%	400일	IM-C.vhdx: 28.79GB / 200GB (14.4%) <span>Dynamic</span> IM-D.vhdx: 4.5GB / 200GB (2.2%) <span>Dynamic</span>
Test01(180.181)	Off	0 GB	0%	0일	Win2012R2-Test01.vhdx: 17.54GB / 100GB (17.5%) <span>Dynamic</span>

SMP-DC01 (샘플IDC) 100.100.180.182

Hyper-V Guest (SAMPLECORP 도메인)

OS <b>Microsoft Windows Server 2022 Standard</b>		버전 <b>10.0.20348</b>	도메인 <b>samplecorp.local</b>
CPU 현재 <b>4%</b>	MEM 현재 <b>76.4%</b>	마지막 부팅 <b>2026-04-15 13:37</b>	가동 일수 <b>26일</b>
제조사 <b>Microsoft Corporation</b>	모델 <b>Virtual Machine</b>	CPU <b>Intel(R) Xeon(R) CPU X5650 @ 2.67GHz</b>	
CPU 구성 <b>1 소켓 / 4 코어 / 4 논리</b>	RAM <b>3.9 GB</b>		

수집 시간: 2026-05-11 13:42

디스크

드라이브	레이블	전체	사용	여유	사용률
C:		99.32 GB	22.72 GB	76.6 GB	22.9%

10.0.10.33 10.0.10.33 연결 실패

Hyper-V Host (IDC 내부, ping 무응답)

[10.0.10.33] Connecting to remote server 10.0.10.33 failed with the following error message : 액세스가 거부되었습니다. For more information, see the about\_Remote\_Troubleshooting Help topic.

수집 시도: 2026-05-11 13:45

## Windows Monitor — 2. 정책 / 계정 / 공유

샘플IDC

IT 운영팀 | 2026년 05월 11일 13:39

 정책 / 계정 / 공유 폴더 (상시)

SMP-PC

10.0.20.50

VMHOST

FileServer

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
로컬	7	-	-	10	30

## 핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	1명	vmadmin

## 로컬 사용자 계정 (2명)

이름	상태	암호 만료	전체 이름
vmadmin	활성	예	
Guest	비활성	아니오 (만료없음)	

## 공유 폴더 (9개)

공유명	경로	설명
C	C:\	
C\$	C:\	기본 공유
H\$	H:\	기본 공유
I	I:\	
I\$	I:\	기본 공유
K	K:\	
K\$	K:\	기본 공유
L\$	L:\	기본 공유
M\$	M:\	기본 공유

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
로컬	10	-	-	10	10

## 핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	3명	Administrator, VMHOST#svc-mon, VMHOST#Domain Admins
Remote Management Users	1명	VMHOST#svc-mon
Event Log Readers	1명	VMHOST#svc-mon
Performance Monitor Users	1명	VMHOST#svc-mon

## 로컬 사용자 계정 (2명)

이름	상태	암호 만료	전체 이름
Administrator	활성	예	
Guest	비활성	아니오 (만료없음)	

## 공유 폴더 (7개)

공유명	경로	설명
C\$	C:\	기본 공유
D\$	D:\	기본 공유
VMHOST-Base	L:\VMHOST-Base	
Install_All	L:\Install_All	
L\$	L:\	기본 공유
Temp	L:\Temp	
X\$	X:\	기본 공유

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
도메인	8	42	-	10	10
로컬	8	42	-	10	10

 AD 복제 상태 / Domain Controllers 정상

파트너/DC	사이트	마지막 성공	실패 정보
SMP-DC01	Default-First-Site-Name	2026-05-11 13:40	—

## 공유 폴더 (3개)

공유명	경로	설명
C\$	C:\W	기본 공유
NETLOGON	C:\Windows\SYSTEM32\sysvol\samplecorp.local\SCRIPTS	Logon server share
SYSVOL	C:\Windows\SYSTEM32\sysvol	Logon server share

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
로컬	9	42	-	10	10

## 핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	2명	vmadmin, CORP-ADMIN
Remote Desktop Users	1명	vmadmin

## 로컬 사용자 계정 (6명)

이름	상태	암호 만료	전체 이름
IME_ADMIN	활성	아니오 (만료없음)	IME_ADMIN
IME_SYSTEM	활성	아니오 (만료없음)	IME_SYSTEM
IME_USER	활성	아니오 (만료없음)	IME_USER
vmadmin	활성	아니오 (만료없음)	vmadmin
CORP-ADMIN	활성	아니오 (만료없음)	
Guest	비활성	아니오 (만료없음)	

## 공유 폴더 (5개)

공유명	경로	설명
C\$	C:\	기본 공유
D\$	D:\	기본 공유
E\$	E:\	기본 공유
F\$	F:\	기본 공유
G\$	G:\	기본 공유

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
로컬	10	-	-	10	10

## 핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	3명	Administrator, VMHOST#svc-mon, VMHOST#Domain Admins

## 로컬 사용자 계정 (2명)

이름	상태	암호 만료	전체 이름
Administrator	활성	예	
Guest	비활성	아니오 (만료없음)	

## 공유 폴더 (3개)

공유명	경로	설명
C\$	C:\	기본 공유
I\$	I:\	기본 공유
K\$	K:\	기본 공유

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
로컬	9	42	-	10	10

## 핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	3명	vmadmin, CORP-ADMIN, ukuser
Remote Desktop Users	2명	vmadmin, ukuser
Performance Monitor Users	2명	NT SERVICE\MSSQLSERVER, NT SERVICE\SQLSERVERAGENT

## 로컬 사용자 계정 (4명)

이름	상태	암호 만료	전체 이름
vmadmin	활성	아니오 (만료없음)	vmadmin
CORP-ADMIN	활성	예	
ukuser	활성	아니오 (만료없음)	ukuser
Guest	비활성	아니오 (만료없음)	

## 공유 폴더 (5개)

공유명	경로	설명
C\$	C:W	기본 공유
D\$	D:W	기본 공유
E\$	E:W	기본 공유
F\$	F:W	기본 공유
G\$	G:W	기본 공유

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
도메인	10	-	-	10	10
로컬	10	-	-	10	10

## AD 복제 상태 / Domain Controllers 정상

파트너/DC	사이트	마지막 성공	실패 정보
VHOST-31	Default-First-Site-Name	2026-05-11 13:39	—

## 핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	4명	svc-mon, Domain Admins, Enterprise Admins, vmadmin
Remote Management Users	1명	svc-mon
Event Log Readers	1명	svc-mon
Performance Monitor Users	1명	svc-mon

## 공유 폴더 (5개)

공유명	경로	설명
C\$	C:\W	기본 공유
J\$	J:\W	기본 공유
K\$	K:\W	기본 공유
NETLOGON	C:\Windows\SYSTEM32\sysvol\WVHOST.LOCAL\WSCRIPTS	Logon server share
SYSVOL	C:\Windows\SYSTEM32\sysvol	Logon server share

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
로컬	9	42	-	10	10

## 핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	1명	vmadmin

## 로컬 사용자 계정 (3명)

이름	상태	암호 만료	전체 이름
vmadmin	활성	예	
sqlservice	활성	아니오 (만료없음)	sqlservice
Guest	비활성	아니오 (만료없음)	

## 공유 폴더 (13개)

공유명	경로	설명
C\$	C:W	기본 공유
D\$	D:W	기본 공유
E\$	E:W	기본 공유
F\$	F:W	기본 공유
G\$	G:W	기본 공유
H\$	H:W	기본 공유
I\$	I:W	기본 공유
J\$	J:W	기본 공유
K\$	K:W	기본 공유
L\$	L:W	기본 공유
M\$	M:W	기본 공유
N\$	N:W	기본 공유
S\$	S:W	기본 공유

비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
로컬	0	42	-	아님	30

핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	2명	REMOTE-A\Administrator, REMOTE-A\remote

로컬 사용자 계정 (6명)

이름	상태	암호 만료	전체 이름
remote	활성	아니오 (만료없음)	
Administrator	비활성	아니오 (만료없음)	
DefaultAccount	비활성	아니오 (만료없음)	
defaultuser0	비활성	아니오 (만료없음)	
Guest	비활성	아니오 (만료없음)	
WDAGUtilityAccount	비활성	예	

공유 폴더 (3개)

공유명	경로	설명
C\$	C:\	기본 공유
D\$	D:\	기본 공유
접속정보	C:\접속정보	

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
도메인	10	-	-	10	10
로컬	10	-	-	10	10

## AD 복제 상태 / Domain Controllers 정상

파트너/DC	사이트	마지막 성공	실패 정보
VHOST-03	Default-First-Site-Name	2026-05-11 13:43	—

## 핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	4명	svc-mon, Domain Admins, Enterprise Admins, vmadmin
Remote Management Users	1명	svc-mon
Event Log Readers	1명	svc-mon
Performance Monitor Users	1명	svc-mon

## 공유 폴더 (9개)

공유명	경로	설명
C\$	C:\	기본 공유
D\$	D:\	기본 공유
I\$	I:\	기본 공유
J\$	J:\	기본 공유
K\$	K:\	기본 공유
I\ntest	D:\I\ntest	
NETLOGON	C:\Windows\SYSVOL\sysvol\VMHOST.local\SCRIPTS	Logon server share
samplepro-ex2016 install	D:\samplepro-ex2016 install	
SYSVOL	C:\Windows\SYSVOL\sysvol	Logon server share

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
로컬	0	42	-	10	10

## 핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	1명	SMP-WEB#vmadmin

## 로컬 사용자 계정 (4명)

이름	상태	암호 만료	전체 이름
vmadmin	활성	아니오 (만료없음)	
DefaultAccount	비활성	아니오 (만료없음)	
Guest	비활성	아니오 (만료없음)	
WDAGUtilityAccount	비활성	예	

## 공유 폴더 (3개)

공유명	경로	설명
C\$	C:\	기본 공유
D\$	D:\	기본 공유
E\$	E:\	기본 공유

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
도메인	0	-	-	20	10
로컬	0	-	-	20	10

 AD 복제 상태 [단독 AD]

## 핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	5명	Domain Admins, Enterprise Admins, Exchange Trusted Subsystem, vadmin, Organization Management

## 공유 폴더 (10개)

공유명	경로	설명
Address	D:\Exchange Server\WV14\Mailbox\address	"Access to address objects"
C\$	C:\	기본 공유
D\$	D:\	기본 공유
Exchange0AB	D:\Exchange Server\WV14\Exchange0AB	OAB Distribution share
F\$	F:\	기본 공유
G\$	G:\	기본 공유
GroupMetrics	D:\Exchange Server\WV14\GroupMetrics	메일 설명 그룹 메트릭 게시 지점
H\$	H:\	기본 공유
NETLOGON	C:\Windows\SYSTEM32\sysvol\samplemail.local\WSCRIPTS	Logon server share
SYSVOL	C:\Windows\SYSTEM32\sysvol	Logon server share

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
로컬	0	-	-	아님	30

## 핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	1명	vmadmin

## 로컬 사용자 계정 (4명)

이름	상태	암호 만료	전체 이름
IME_ADMIN	활성	아니오 (만료없음)	IME_ADMIN
IME_USER	활성	아니오 (만료없음)	IME_USER
vmadmin	활성	예	
Guest	비활성	아니오 (만료없음)	

## 공유 폴더 (4개)

공유명	경로	설명
C\$	C:\	기본 공유
D\$	D:\	기본 공유
E\$	E:\	기본 공유
F\$	F:\	기본 공유

비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
로컬	0	42	-	아님	30

핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	2명	REMOTE-B\Administrator, REMOTE-B\remote

로컬 사용자 계정 (6명)

이름	상태	암호 만료	전체 이름
remote	활성	아니오 (만료없음)	
Administrator	비활성	아니오 (만료없음)	
DefaultAccount	비활성	아니오 (만료없음)	
defaultuser0	비활성	아니오 (만료없음)	
Guest	비활성	아니오 (만료없음)	
WDAGUtilityAccount	비활성	예	

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
로컬	0	42	-	아님	30

## 핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	2명	REMOTE-C\Administrator, REMOTE-C\remote

## 로컬 사용자 계정 (6명)

이름	상태	암호 만료	전체 이름
remote	활성	아니오 (만료없음)	
Administrator	비활성	아니오 (만료없음)	
DefaultAccount	비활성	아니오 (만료없음)	
defaultuser0	비활성	아니오 (만료없음)	
Guest	비활성	아니오 (만료없음)	
WDAGUtilityAccount	비활성	예	

## 공유 폴더 (2개)

공유명	경로	설명
C\$	C:\	기본 공유
Temp	C:\Temp	

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
로컬	10	-	-	10	10

## 핵심 그룹 멤버

그룹	멤버 수	멤버
Administrators	3명	Administrator, VMHOST#svc-mon, VMHOST#Domain Admins

## 로컬 사용자 계정 (2명)

이름	상태	암호 만료	전체 이름
Administrator	활성	예	
Guest	비활성	아니오 (만료없음)	

## 공유 폴더 (6개)

공유명	경로	설명
C\$	C:\W	기본 공유
D\$	D:\W	기본 공유
E\$	E:\W	기본 공유
I\$	I:\W	기본 공유
J\$	J:\W	기본 공유
K\$	K:\W	기본 공유

## 비밀번호 / 잠금 정책

구분	최소 길이	최대 사용 기간	기록 길이	잠금 임계값	잠금 기간(분)
도메인	8	42	-	10	10
로컬	8	42	-	10	10

## AD 복제 상태 / Domain Controllers 정상

파트너/DC	사이트	마지막 성공	실패 정보
SMP-DC02	Default-First-Site-Name	2026-05-11 13:42	—

## 공유 폴더 (3개)

공유명	경로	설명
C\$	C:\W	기본 공유
NETLOGON	C:\Windows\SYSTEM32\sysvol\samplecorp.local\SCRIPTS	Logon server share
SYSVOL	C:\Windows\SYSTEM32\sysvol	Logon server share

## Windows Monitor — 3. 시스템 / 보안 로그

샘플IDC

IT 운영팀 | 2026년 05월 11일 13:39

물리 SMP-PC 10.0.20.50

보안 위협 통합 외부 IP 1개 현재 접속 1개

외부 IP	로그온 실패 (SecEvent)	IIS 401	접속 상태	Local Port	Remote Port	프로세스	국가	회사명 (ISP)
20.41.64.68	-	-	● 접속 중	51921	443	MonAgentManager	KR South Korea	Microsoft Corporation

시스템 이벤트 (Critical / Error) 2026-05-04 ~ 2026-05-11 (8일) 1종 (총 13건)

최근 발생	수준	소스	EventID	메시지
2026-05-11 12:06	오류	NETLOGON 13회	5719	다음과 같은 이유로 인해 COMPANY 도메인에 있는 도메인 컨트롤러로 이 컴퓨터의 보안 세션을 설정할 수 없습니다. 지금은 로그인 요청에 서비스할 수 있는 로그인 서버가 없습니다. 이로 인해 인증 문제가 발생할 수 있습니다. 이 컴퓨터가 네트워크에 연결되어 있는지 확인하십시오. 문제가 계속되면 도메인 관리자에게 문의해 보십시오. 추가 정보 이 컴퓨터가 지정한 도메인의 도메인 컨트롤러이면, 이 컴퓨터는 지정한 도메인 내에서 주 도메인 컨트롤러 에뮬레이터에 보안 세션을 설정합니다. 그렇지 않으면, 이 컴퓨터는 지정한 도메인에 있는 임의의 도메인 컨트롤러에 보안 세션을 설정합니다.

원인: 도메인 로그인 서비스 오류 조치: 도메인 컨트롤러 연결 확인, Netlogon 서비스 재시작

최근 발생	유형	EventID	메시지 / 침입 정보						
2026-05-11 11:56	로그온 실패 14회	4625	<p>계정을 로그인하지 못했습니다. 주체: 보안 ID: S-1-0-0 계정 이름: - 계정 도메인: - 로그인 ID: 0x0 로그인 유형: 3 로그인을 실패한 계정: 보안 ID: S-1-0-0 계정 이름: Administrator 계정 도메인: INF-AIHOST 오류 정보: 오류 이유: 알 수 없는 사용자 이름 또는 잘못된 암호를 사용했습니다. 상태: 0xC000006D 하위 상태: 0xC0000064 프로세스 정보: 호출자 프로세스 ID: 0x0 호출자 프로세스 이름: - 네트워크 정보: 워크스테이션 이름: INF-AIHOST 원본 네트워크 주소: 192.168.10.13 원본 포트: 49740 인증 세부 정보: 로그인 프로세스: NtLmSsp 인증 패키지: NTLM 전송된 서비스: - 패키지 이름(NTLM 전용): - 키 길이: 0 이 이벤트는 로그인 요청이 실패할 때 액세스하려고 했던 컴퓨터에 생성됩니다. 주체 필드는 로그인을 요청한 로컬 시스템의 계정을 나타냅니다. 이것은 주로 서버 서비스와 같은 서비스 또는 Winlogon.exe나 Services.exe와 같은 로컬 프로세스입니다. 로그인 유형 필드는 요청한 로그인의 유형을 나타냅니다. 가장 일반적인 유형은 2(대화식)와 3(네트워크)입니다. 프로세스 정보 필드는 시스템에서 로그인을 요청한 계정과 프로세스를 나타냅니다. 네트워크 정보 필드는 원격 로그인 요청이 시작된 위치를 나타냅니다. 워크스테이션 이름은 항상 사용할 수 있는 것은 아니며 어떤 경우에는 비워 둘 수도</p> <table border="1"> <thead> <tr> <th>침입 IP</th> <th>계정</th> <th>워크스테이션</th> </tr> </thead> <tbody> <tr> <td>192.168.10.13 14회</td> <td>-</td> <td>INF-AIHOST</td> </tr> </tbody> </table> <p>📌 로그인 실패 계정별 (1종) Administrator 14회</p>	침입 IP	계정	워크스테이션	192.168.10.13 14회	-	INF-AIHOST
침입 IP	계정	워크스테이션							
192.168.10.13 14회	-	INF-AIHOST							

**원인:** 반복적인 로그인 실패 — 무차별 대입(Brute-force) 또는 자격증명 오류  
**조치:** 계정 잠금 정책 적용, 소스 IP 방화벽 차단, RDP 포트 변경 검토

### ⚠️ 침입 시도 IP 및 조치 방법

감지된 IP: 192.168.10.13

- **즉시 차단 (PowerShell):** `New-NetFirewallRule -DisplayName 'Block_<IP>' -Direction Inbound -RemoteAddress <IP> -Action Block`
- **이벤트 확인:** 이벤트 뷰어 → Windows 로그 → 보안 → EventID 4625 필터
- **계정 잠금 확인:** `net user <계정명>` 잠금 해제: `net user <계정명> /active:yes`
- **RDP 포트 변경 권장 (기본 3389 → 변경):** `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\WRDP-Tcp → PortNumber`
- **계정 잠금 정책 설정:** secpol.msc → 계정 정책 → 계정 잠금 임계값 (5회 권장)
- **원격 데스크톱 NLA 강제:** `Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinAuth' -Name 'SecurityLayer' -Value 2`

물리

VHOST-DR01

100.100.180.190

보안 위협 통합 외부 IP 1개

현재 접속 1개

외부 IP	로그온 실패 (SecEvent)	IIS 401	접속 상태	Local Port	Remote Port	프로세스	국가	회사명 (ISP)
210.91.34.58	-	-	● 접속 중	4489, 5985	53582, 54685, 56413, 56414, 56415	PID:0	KR South Korea	Korea Telecom

시스템 이벤트 (Critical / Error)

2026-05-04 ~ 2026-05-11 (8일)

1종 (총 21건)

최근 발생	수준	소스	EventID	메시지
2026-05-11 12:57	오류	Microsoft-Windows-GroupPolicy (21회)	1080	그룹 정책을 처리하지 못했습니다. Active Directory 조직 단위 계층 구조를 검색하지 못했습니다. 자세한 내용은 이벤트 세부 정보를 참조하세요.

원인: 시스템 이벤트 오류 조치: 이벤트 상세 메시지 확인 후 해당 서비스 재시작

VM

SMP-DC02 (샘플IDC)

100.100.180.187

보안 위협 통합

외부 IP 2개

현재 접속 2개

외부 IP	로그온 실패 (SecEvent)	IIS 401	접속 상태	Local Port	Remote Port	프로세스	국가	회사명 (ISP)
168.126.63.1	-	-	● 접속 중	54724	53	dns	KR South Korea	Korea Telecom
168.126.63.2	-	-	● 접속 중	54747, 54748, 54750, 54751, 54758, 54759, 54761	53	dns	KR South Korea	Korea Telecom

시스템 이벤트 (Critical / Error)

2026-05-04 ~ 2026-05-11 (8일)

1일 1회 초과 반복 이벤트 없음

보안 이벤트 (계정 변경 + 로그온 실패)

2026-05-04 ~ 2026-05-11 (8일)

1건

최근 발생	유형	EventID	메시지 / 침입 정보
2026-05-07 14:54	계정 비활성화	4725	사용자 계정을 사용할 수 없습니다. 주체: 보안 ID: S-1-5-21-2000478354-1123561945-725345543-500 계정 이름: vmadmin 계정 도메인: SAMPLECORP 로그인 ID: 0x1935B01A 대상 계정: 보안 ID: S-1-5-21-2000478354-1123561945-725345543-7605 계정 이름: SMP-WEB\$ 계정 도메인: SAMPLECORP

원인: 사용자 계정 비활성화 조치: 비활성화 주체 및 사유 확인

⚠ 시스템 이벤트 (Critical / Error) 2026-05-04 ~ 2026-05-11 (8일) 1종 (총 26건)

최근 발생	수준	소스	EventID	메시지
2026-05-11 13:10	오류	Schannel 26회	36887	원격 끝점에서 경고를 받았습니다. 경고 코드에 정의된 TLS 프로토콜은 70입니다.

**원인:** 시스템 이벤트 오류 **조치:** 이벤트 상세 메시지 확인 후 해당 서비스 재시작

⚠ 시스템 이벤트 (Critical / Error) 2026-05-04 ~ 2026-05-11 (8일)

1일 1회 초과 반복 이벤트 없음

🛡 보안 위협 통합 외부 IP 3개 🔴 현재 접속 3개

외부 IP	로그온 실패 (SecEvent)	IIS 401	접속 상태	Local Port	Remote Port	프로세스	국가	회사명 (ISP)
1.244.116.18	-	-	🔴 접속 중	49486	80	SmartUpdaterClient	KR South Korea	SK Broadband Co Ltd
218.48.234.167	-	-	🔴 접속 중	2639	13371, 16285, 16300, 16364, 16471, 16567, 16854, 18837, 19267, 19384, 19749, 19783, 20421, 28698, 28843, 29642, 30080, 30336, 41290, 41715, 41975, 42069, 42260, 42758, 42772, 44139, 52660, 52663, 52669, 53301, 53669, 53682, 53683, 53685, 57513, 58153, 58185, 58249, 62778, 63496, 63497, 63836, 63868	SDB_Server_plus_64	KR South Korea	SK Broadband Co Ltd
211.115.106.73	-	-	🔴 접속 중	49585	80	ASDSvc	KR South Korea	LG DACOM Corporation

⚠ 시스템 이벤트 (Critical / Error) 2026-05-04 ~ 2026-05-11 (8일)

1일 1회 초과 반복 이벤트 없음

물리 VHOST-03 10.0.10.13

⚠ 시스템 이벤트 (Critical / Error) 2026-05-04 ~ 2026-05-11 (8일)

1일 1회 초과 반복 이벤트 없음

VM SMP-SQL (샘플IDC) 10.0.30.250

⚠ 시스템 이벤트 (Critical / Error) 2026-05-04 ~ 2026-05-11 (8일)

1일 1회 초과 반복 이벤트 없음

VM REMOTE-A (샘플IDC) 10.0.30.55

🛡 보안 위협 통합 외부 IP 3개 🔴 현재 접속 3개

외부 IP	로그온 실패 (SecEvent)	IIS 401	접속 상태	Local Port	Remote Port	프로세스	국가	회사명 (ISP)
4.213.25.240	-	-	🔴 접속 중	51626	443	svchost	IN India	Microsoft Corporation
20.189.173.3	-	-	🔴 접속 중	54922	443	OneDrive	US United States	Microsoft Corporation
23.63.226.36	-	-	🔴 접속 중	54921	443	svchost	JP Japan	Akamai Technologies, Inc.

⚠ 시스템 이벤트 (Critical / Error) 2026-05-04 ~ 2026-05-11 (8일) 1종 (총 27건)

최근 발생	수준	소스	EventID	메시지
2026-05-11 13:38	오류	ESENT (27회)	455	svchost (9716,R,98) TILEREPOSITORY-1-5-18: 로그 파일 C:\WINDOWS\system32\config\systemprofile\AppData\Local\TileDataLayer\Database\EDB.log을(를) 여는 동안 -1023 (0xffffc01) 오류가 발생했습니다.

원인: 시스템 이벤트 오류 조치: 이벤트 상세 메시지 확인 후 해당 서비스 재시작

물리 VHOST-31 10.0.10.31

⚠ 시스템 이벤트 (Critical / Error) 2026-05-04 ~ 2026-05-11 (8일)

1일 1회 초과 반복 이벤트 없음

VM

SMP-WEB

(샘플IDC)

100.100.180.184

보안 위협 통합

외부 IP 1개

현재 접속 1개

외부 IP	로그온 실패 (SecEvent)	IIS 401	접속 상태	Local Port	Remote Port	프로세스	국가	회사명 (ISP)
168.126.63.2	-	-	● 접속 중	62299, 62308, 62309, 62310	53	dns	KR South Korea	Korea Telecom

⚠ 시스템 이벤트 (Critical / Error)

2026-05-04 ~ 2026-05-11 (8일)

1종 (총 28건)

최근 발생	수준	소스	EventID	메시지
2026-05-11 04:59	오류	Schannel 28회	36874	원격 클라이언트 응용 프로그램으로부터 TLS 1.2 연결 요청을 받았지만 클라이언트 응용 프로그램에서 지원하는 암호화 그룹 중 어떤 것도 서버가 지원하지 않습니다. TLS 연결 요청이 실패했습니다. SSPI 클라이언트 프로세스가 SYSTEM(PID: 4)입니다.

**원인:** 시스템 이벤트 오류 **조치:** 이벤트 상세 메시지 확인 후 해당 서비스 재시작

최근 발생	유형	Event ID	메시지 / 침입 정보												
2026-05-07 15:08	관리자 암호 재설정	4724	계정 암호를 다시 설정하려고 했습니다. 주체: 보안 ID: S-1-5-21-1158285041-1757169806-1361681515-500 계정 이름: Administrator 계정 도메인: SMP-WEB 로그인 ID: 0x6342D 대상 계정: 보안 ID: S-1-5-21-1158285041-1757169806-1361681515-500 계정 이름: vadmin 계정 도메인: SMP-WEB												
<b>원인:</b> 관리자에 의한 비밀번호 재설정			<b>조치:</b> 재설정 주체 및 대상 계정 확인												
2026-05-07 15:08	계정 변경	4738	사용자 계정을 변경했습니다. 주체: 보안 ID: S-1-5-21-1158285041-1757169806-1361681515-500 계정 이름: Administrator 계정 도메인: SMP-WEB 로그인 ID: 0x6342D 대상 계정: 보안 ID: S-1-5-21-1158285041-1757169806-1361681515-500 계정 이름: vadmin 계정 도메인: SMP-WEB 변경된 특성: SAM 계정 이름: vadmin 표시 이름: <값을 설정하지 않음> UPN(사용자 계정 이름): - 홈 디렉터리: <값을 설정하지 않음> 홈 드라이브: <값을 설정하지 않음> 스크립트 경로: <값을 설정하지 않음> 프로필 경로: <값을 설정하지 않음> 사용자 워크스테이션: <값을 설정하지 않음> 마지막 암호 설정: 2026-05-07 오후 3:08:37 계정 만료: <작업하지 않음> 기본 그룹 ID: 513 위임하도록 허용된 대상: - 이전 UAC 값: 0x210 새 UAC 값: 0x210 사용자 계정 컨트롤: - 사용자 매개 변수: - SID 기록: - 로그인 시간: 모두 추가 정보: 권한: -												
<b>원인:</b> 보안 이벤트			<b>조치:</b> 이벤트 상세 확인 후 필요 시 계정 잠금 및 IP 차단												
2026-05-07 15:04	로그인 실패 39회	4625	계정을 로그인하지 못했습니다. 주체: 보안 ID: S-1-0-0 계정 이름: - 계정 도메인: - 로그인 ID: 0x0 로그인 유형: 3 로그인을 실패한 계정: 보안 ID: S-1-0-0 계정 이름: vadmin 계정 도메인: MicrosoftAccount 오류 정보: 오류 이유: 알 수 없는 사용자 이름 또는 잘못된 암호를 사용했습니다. 상태: 0xC000006D 하위 상태: 0xC0000064 프로세스 정보: 호출자 프로세스 ID: 0x0 호출자 프로세스 이름: - 네트워크 정보: 워크스테이션 이름: JAMES-LENOVO 원본 네트워크 주소: 210.91.34.58 원본 포트: 0 인증 세부 정보: 로그인 프로세스: NtLmSsp 인증 패키지: NTLM 전송된 서비스: - 패키지 이름 (NTLM 전용): - 키 길이: 0 이 이벤트는 로그인 요청이 실패할 때 액세스하려고 했던 컴퓨터에 생성됩니다. 주체 필드는 로그인을 요청한 로컬 시스템의 계정을 나타냅니다. 이것은 주로 서버 서비스와 같은 서비스 또는 Winlogon.exe나 Services.exe와 같은 로컬 프로세스입니다. 로그인 유형 필드는 요청한 로그인의 유형을 나타냅니다. 가장 일반적인 유형은 2(대화식)와 3(네트워크)입니다. 프로세스 정보 필드는 시스템에서 로그인을 요청한 계정과 프로세스를 나타냅니다. 네트워크 정보 필드는 원격 로그인 요청이 시작된 위치를 나타냅니다. 워크스테이션 이름은 항상 사용할 수 있는 것은 아니며 어떤 경우에는 비워 둘 수도												
<table border="1"> <thead> <tr> <th>침입 IP</th> <th>계정</th> <th>워크스테이션</th> </tr> </thead> <tbody> <tr> <td>210.91.34.58 3회</td> <td>-</td> <td>JAMES-LENOVO</td> </tr> <tr> <td>100.100.180.182 10회</td> <td>-</td> <td>SMP-DC01</td> </tr> <tr> <td>100.100.180.187 15회</td> <td>-</td> <td>SMP-DC02</td> </tr> </tbody> </table>				침입 IP	계정	워크스테이션	210.91.34.58 3회	-	JAMES-LENOVO	100.100.180.182 10회	-	SMP-DC01	100.100.180.187 15회	-	SMP-DC02
침입 IP	계정	워크스테이션													
210.91.34.58 3회	-	JAMES-LENOVO													
100.100.180.182 10회	-	SMP-DC01													
100.100.180.187 15회	-	SMP-DC02													
<b>원인:</b> 반복적인 로그인 실패 — 무차별 대입(Brute-force) 또는 자격증명 오류			<b>조치:</b> 계정 잠금 정책 적용, 소스 IP 방화벽 차단, RDP 포트 변경 검토												
2026-05-07 14:44	계정 생성	4720	사용자 계정을 만들었습니다. 주체: 보안 ID: S-1-5-18 계정 이름: SMP-WEB\$ 계정 도메인: SAMPLECORP 로그인 ID: 0x3E7 새 계정: 보안 ID: S-1-5-21-1158285041-1757169806-1361681515-504 계정 이름: WDAGUtilityAccount 계정 도메인: SMP-WEB 특성: SAM 계정 이름: WDAGUtilityAccount 표시 이름: <값을 설정하지 않음> UPN(사용자 계정 이름): - 홈 디렉터리: <값을 설정하지 않음> 홈 드라이브: <값을 설정하지 않음> 스크립트 경로: <값을 설정하지 않음> 프로필 경로: <값을 설정하지 않음> 사용자 워크스테이션: <값을 설정하지 않음> 마지막 암호 설정: <작업하지 않음> 계정 만료: <작업하지 않음> 기본 그룹 ID: 513 위임하도록 허용된 대상: - 이전 UAC 값: 0x0 새 UAC 값: 0x15 사용자 계정 컨트롤: Account 사용 안 함 '암호 불필요' - 사용함 '일반 계정' - 사용함 사용자 매개 변수: <값을 설정하지 않음> SID 기록: - 로그인 시간: 모두 추가 정보: 권한: -												

최근 발생      유형      Event ID      메시지 / 침입 정보

**원인:** 새 사용자 계정이 생성됨      **조치:** 승인되지 않은 계정 생성 여부 확인, 불필요한 경우 즉시 삭제

### ⚠ 침입 시도 IP 및 조치 방법

감지된 IP:    210.91.34.58    100.100.180.182    100.100.180.187

- **즉시 차단 (PowerShell):** `New-NetFirewallRule -DisplayName 'Block_<IP>' -Direction Inbound -RemoteAddress <IP> -Action Block`
- **이벤트 확인:** 이벤트 뷰어 → Windows 로그 → 보안 → EventID 4625 필터
- **계정 잠금 확인:** `net user <계정명>`    잠금 해제: `net user <계정명> /active:yes`
- **RDP 포트 변경 권장 (기본 3389 → 변경):** `HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\WRDP-Tcp` → PortNumber
- **계정 잠금 정책 설정:** secpol.msc → 계정 정책 → 계정 잠금 임계값 (5회 권장)
- **원격 데스크톱 NLA 강제:** `Set-ItemProperty 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinAuth' -Name 'SecurityLayer' -Value 2`

보안 위협 통합 외부 IP 15개 현재 접속 14개

외부 IP	로그 온 실 패 (SecE vent)	IIS 401	접속 상태	Local Port	Remote Port	프로세스	국가	회사명 (ISP)
220.116.0.243	-	324 건	● 접속 중	443	33244, 38410, 39532, 57111, 57114, 57117, 57119, 57123, 57124, 57125, 57128, 57279, 57280, 63857, 63860, 63863, 63864, 63865, 63866, 63867, 63868, 63946, 63947	System	KR South Korea	Korea Telecom
1.232.10.180	-	34 건	● 접속 중	443	55315, 55316, 55317, 55318, 58686, 58687	System	KR South Korea	SK Broadband Co Ltd
68.36.105.154	-	12 건	-	-	-	-	US United States	Comcast Cable Communications, LLC
168.126.63.2	-	-	● 접속 중	49881	53	dns	KR South Korea	Korea Telecom
191.36.152.28	-	-	● 접속 중	587	33982	EdgeTransport	BR Brazil	VIPTURBO COMÉRCIO & SERVIÇOS DE INFORMÁTICA LTDA
136.228.168.12	-	-	● 접속 중	25	63667	EdgeTransport	MM Myanmar	Myanma Post & Telecommunication
35.231.154.163	-	-	● 접속 중	443	17664	System	US United States	Google LLC
211.32.93.133	-	-	● 접속 중	25	56639	EdgeTransport	KR South Korea	kbcard
20.9.82.33	-	-	● 접속 중	80	37071	System	US United States	Microsoft Corporation
211.234.194.186	-	-	● 접속 중	443	35594, 46844, 46860, 46866	System	KR South Korea	SK Telecom
118.235.13.83	-	-	● 접속 중	443	61039	System	KR South Korea	Korea Telecom
203.247.149.244	-	-	● 접속 중	443	10002	System	KR South Korea	LG CNS
211.234.181.140	-	-	● 접속 중	443	18362	System	KR South Korea	SK Telecom
211.234.227.168	-	-	● 접속 중	443	59410	System	KR South Korea	SK Telecom
168.126.63.1	-	-	● 접속 중	49882	53	dns	KR South Korea	Korea Telecom

중지된 서비스 (자동 시작 권장):

서비스명	표시 이름	상태	시작 유형
MSExchangeImap4	Microsoft Exchange IMAP4	Stopped	
MSExchangeMonitoring	Microsoft Exchange 모니터링	Stopped	

최근 24h Application 오류 (상위 10건 / 총 200건):

발생 시각	소스	EventID	건수	메시지
05-11 13:37	MSExchangeTransport	12014	51회	Microsoft Exchange가 로컬 컴퓨터의 개인 저장소에서 도메인 이름 SMP-EX02.samplemail.local이(가) 포함된 인증서를 찾을 수 없습니다. 그러므로 FQDN 매개 변수 SMP-EX02.samplemail.local이(가) 있는 커넥터 Client SMP-EX02에 대해 STARTTLS SMTP 동사를 지원할 수 없습니다. 커넥터의 FQDN을 지정하지 않은 경우 컴퓨터의 FQDN이 사용됩니다. 커넥터 구성 및 설치된 인증서를 확인하여 해당 FQDN에 대한 도메인 이름이 포함된 인증서가 있는지 확인하십시오. 이 인
05-11 13:37	MSExchangeTransport	12014	50회	Microsoft Exchange가 로컬 컴퓨터의 개인 저장소에서 도메인 이름 mail.sampleidc.net이(가) 포함된 인증서를 찾을 수 없습니다. 그러므로 FQDN 매개 변수 mail.sampleidc.net이(가) 있는 커넥터 ToInternet에 대해 STARTTLS SMTP 동사를 지원할 수 없습니다. 커넥터의 FQDN을 지정하지 않은 경우 컴퓨터의 FQDN이 사용됩니다. 커넥터 구성 및 설치된 인증서를 확인하여 해당 FQDN에 대한 도메인 이름이 포함된 인증서가 있는지 확인하십시오. 이 인증서가 있는 경우 Enabl
05-11 13:42	MSExchangeTransport	12014	48회	Microsoft Exchange가 로컬 컴퓨터의 개인 저장소에서 도메인 이름 SMP-EX02.samplemail.local이(가) 포함된 인증서를 찾을 수 없습니다. 그러므로 FQDN 매개 변수 SMP-EX02.samplemail.local이(가) 있는 커넥터 Default SMP-EX02에 대해 STARTTLS SMTP 동사를 지원할 수 없습니다. 커넥터의 FQDN을 지정하지 않은 경우 컴퓨터의 FQDN이 사용됩니다. 커넥터 구성 및 설치된 인증서를 확인하여 해당 FQDN에 대한 도메인 이름이 포함된 인증서가 있는지 확인하십시오. 이
05-11 13:42	MSExchangeTransport	12015	47회	내부 전송 인증서가 만료되었습니다. 지문:758B4F91CD68375A350B3D891C57EDA01018A952
05-11 13:28	MSExchangeTransport	12014	3회	Microsoft Exchange가 로컬 컴퓨터의 개인 저장소에서 도메인 이름 SMP-EX02.samplemail.local이(가) 포함된 인증서를 찾을 수 없습니다. 그러므로 FQDN 매개 변수 SMP-EX02.samplemail.local이(가) 있는 커넥터 Port26에 대해 STARTTLS SMTP 동사를 지원할 수 없습니다. 커넥터의 FQDN을 지정하지 않은 경우 컴퓨터의 FQDN이 사용됩니다. 커넥터 구성 및 설치된 인증서를 확인하여 해당 FQDN에 대한 도메인 이름이 포함된 인증서가 있는지 확인하십시오. 이 인증서가 있는 경우
05-11 01:03	MSExchangeAL	8365	1회	GUID가 16BBCB650E5D0B44AD480DB2EC0ACD0C인 Exchange Server 개체에서 보안 설명자를 읽을 수 없습니다. 결과적으로 로컬 Exchange Server에서 프록시 주소 계산 RPC 인터페이스를 사용할 수 없습니다.

▲ 시스템 이벤트 (Critical / Error)

2026-05-04 ~ 2026-05-11 (8일)

2중 (총 20건)

최근 발생	수준	소스	EventID	메시지
2026-05-11 13:43	오류	Schannel 10회	36874	원격 클라이언트 응용 프로그램으로부터 TLS 1.2 연결 요청을 받았으나 클라이언트 응용 프로그램이 지원하는 암호 그룹 중 어떤 것도 서버가 지원하지 않습니다. SSL 연결 요청이 실패했습니다.
<b>원인:</b> 시스템 이벤트 오류 <b>조치:</b> 이벤트 상세 메시지 확인 후 해당 서비스 재시작				
2026-05-11 13:43	오류	Schannel 10회	36888	다음 경고가 발생했습니다. 40. 내부 오류 상태는 1205입니다.
<b>원인:</b> 시스템 이벤트 오류 <b>조치:</b> 이벤트 상세 메시지 확인 후 해당 서비스 재시작				

**보안 이벤트 (계정 변경 + 로그인 실패) 2026-05-04 ~ 2026-05-11 (8일) 1종 (총 1000건)**

최근 발생	유형	Event ID	메시지 / 침입 정보															
2026-05-11 13:46	로그온 실패 1000회	4625	<p>계정을 로그인하지 못했습니다. 주체: 보안 ID: S-1-5-20 계정 이름: SMP-EX02\$ 계정 도메인: MAILHOST 로그인 ID: 0x3e4 로그인 유형: 8 로그온을 실패한 계정: 보안 ID: S-1-0-0 계정 이름: user-mgr1 계정 도메인: 오류 정보: 오류 이유: 알 수 없는 사용자 이름 또는 잘못된 암호를 사용했습니다. 상태: 0xc000006d 하위 상태: 0xc0000064 프로세스 정보: 호출자 프로세스 ID: 0x1008 호출자 프로세스 이름: D:\Exchange Server\WV14\ClientAccess\PopImap\Microsoft.Exchange.Pop3.exe 네트워크 정보: 워크스테이션 이름: SMP-EX02 원본 네트워크 주소: - 원본 포트: - 인증 세부 정보: 로그인 프로세스: Advapi 인증 패키지: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0 전송된 서비스: - 패키지 이름(NTLM 전용): - 키 길이: 0 이 이벤트는 로그인 요청이 실패할 때 액세스하려고 했던 컴퓨터에 생성됩니다. 주체 필드는 로그온을 요청한 로컬 시스템의 계정을 나타냅니다. 이것은 주로 서버 서비스와 같은 서비스 또는 Winlogon.exe나 Services.exe와 같은 로컬 프로세스입니다. 로그인 유형 필드는 요청한 로그온의 유형을 나타냅니다. 가장 일반적인 유형은 2(대화식)과 3(네트워크)입니다. 프로세스 정보 필드는 시스템에서 로그온을 요청한 계정과 프로</p> <table border="1"> <thead> <tr> <th>침입 IP</th> <th>계정</th> <th>워크스테이션</th> </tr> </thead> <tbody> <tr> <td>-</td> <td>16회</td> <td>DESKTOP-MCU4J95</td> </tr> <tr> <td>-</td> <td>9회</td> <td>윤동섭</td> </tr> </tbody> </table> <p>로그온 실패 계정별 (2종)</p> <table border="1"> <tbody> <tr> <td>chang3103@corp-mac.local</td> <td>dsyun@corp-mac.local</td> <td>9회</td> </tr> <tr> <td colspan="2"></td> <td>16회</td> </tr> </tbody> </table>	침입 IP	계정	워크스테이션	-	16회	DESKTOP-MCU4J95	-	9회	윤동섭	chang3103@corp-mac.local	dsyun@corp-mac.local	9회			16회
침입 IP	계정	워크스테이션																
-	16회	DESKTOP-MCU4J95																
-	9회	윤동섭																
chang3103@corp-mac.local	dsyun@corp-mac.local	9회																
		16회																

**원인:** 반복적인 로그인 실패 — 무차별 대입(Brute-force) 또는 자격증명 오류  
**조치:** 계정 잠금 정책 적용, 소스 IP 방화벽 차단, RDP 포트 변경 검토

**VM SMP-SMTP (샘플IDC) 200.200.227.226**

**시스템 이벤트 (Critical / Error) 2026-05-04 ~ 2026-05-11 (8일) 2종 (총 28건)**

최근 발생	수준	소스	Event ID	메시지
2026-05-10 22:51	오류	Schannel 14회	36888	경고 발생했으며 원격 끝점으로 전송되었습니다. 이 경고로 인해 연결이 종료될 수 있습니다. 오류 코드에 정의된 TLS 프로토콜은 40입니다. Windows Schannel 오류 상태는 1205입니다.
<p><b>원인:</b> 시스템 이벤트 오류 <b>조치:</b> 이벤트 상세 메시지 확인 후 해당 서비스 재시작</p>				
2026-05-10 22:51	오류	Schannel 14회	36874	원격 클라이언트 응용 프로그램으로부터 TLS 1.2 연결 요청을 받았으나 클라이언트 응용 프로그램이 지원하는 암호 그룹 중 어떤 것도 서버가 지원하지 않습니다. SSL 연결 요청이 실패했습니다.
<p><b>원인:</b> 시스템 이벤트 오류 <b>조치:</b> 이벤트 상세 메시지 확인 후 해당 서비스 재시작</p>				

VM REMOTE-B (샘플IDC) 10.0.30.56

보안 위협 통합 외부 IP 1개 현재 접속 1개

외부 IP	로그온 실패 (SecEvent)	IIS 401	접속 상태	Local Port	Remote Port	프로세스	국가	회사명 (ISP)
4.213.25.242	-	-	● 접속 중	49712	443	svchost	IN India	Microsoft Corporation

시스템 이벤트 (Critical / Error) 2026-05-04 ~ 2026-05-11 (8일) 1종 (총 23건)

최근 발생	수준	소스	EventID	메시지
2026-05-11 13:42	오류	ESENT 23회	455	svchost (8780,R,98) TILEREPOSITORYS-1-5-18: 로그 파일 C:\WINDOWS\system32\config\systemprofile\AppData\Local\TileDataLayer\Database\EDB.log(를) 여는 동안 -1023 (0xffffc01) 오류가 발생했습니다.

원인: 시스템 이벤트 오류 조치: 이벤트 상세 메시지 확인 후 해당 서비스 재시작

VM REMOTE-C (샘플IDC) 10.0.30.57

보안 위협 통합 외부 IP 1개 현재 접속 1개

외부 IP	로그온 실패 (SecEvent)	IIS 401	접속 상태	Local Port	Remote Port	프로세스	국가	회사명 (ISP)
4.213.25.240	-	-	● 접속 중	54124	443	svchost	IN India	Microsoft Corporation

시스템 이벤트 (Critical / Error) 2026-05-04 ~ 2026-05-11 (8일) 1종 (총 30건)

최근 발생	수준	소스	EventID	메시지
2026-05-11 13:46	오류	ESENT 30회	455	svchost (8348,R,98) TILEREPOSITORYS-1-5-18: 로그 파일 C:\WINDOWS\system32\config\systemprofile\AppData\Local\TileDataLayer\Database\EDB.log(를) 여는 동안 -1023 (0xffffc01) 오류가 발생했습니다.

원인: 시스템 이벤트 오류 조치: 이벤트 상세 메시지 확인 후 해당 서비스 재시작

물리 VHOST-32 10.0.10.32

시스템 이벤트 (Critical / Error) 2026-05-04 ~ 2026-05-11 (8일) 1종 (총 27건)

최근 발생	수준	소스	EventID	메시지
2026-05-11 12:38	오류	Microsoft-Windows-GroupPolicy 27회	1030	그룹 정책을 처리하지 못했습니다. 이 사용자 또는 컴퓨터의 새 그룹 정책 설정을 검색하려고 했습니다. 오류 코드 및 설명은 세부 정보 탭을 참조하세요. 다음 새로 고침 주기에 자동으로 이 작업이 다시 시도됩니다. 새 그룹 정책 개체와 설정을 검색하려면 도메인에 가입한 컴퓨터에서 도메인 컨트롤러에 대한 적절한 이름 확인 및 네트워크 연결이 이루어져야 합니다. 그룹 정책이 성공하면 이벤트가 기록됩니다.

원인: 시스템 이벤트 오류 조치: 이벤트 상세 메시지 확인 후 해당 서비스 재시작

☑ 보안 위협 통합 외부 IP 2개 ● 현재 접속 2개

외부 IP	로그온 실패 (SecEvent)	IIS 401	접속 상태	Local Port	Remote Port	프로세스	국가	회사명 (ISP)
168.126.63.1	-	-	● 접속 중	52484, 52512	53	dns	KR South Korea	Korea Telecom
168.126.63.2	-	-	● 접속 중	52482	53	dns	KR South Korea	Korea Telecom

⚠ 시스템 이벤트 (Critical / Error) 2026-05-04 ~ 2026-05-11 (8일)

1일 1회 초과 반복 이벤트 없음

🔒 보안 이벤트 (계정 변경 + 로그인 실패) 2026-05-04 ~ 2026-05-11 (8일) 3종 (총 5건)

최근 발생	유형	EventID	메시지 / 침입 정보
2026-05-06 14:06	계정 활성화	4722	사용자 계정을 사용할 수 있습니다. 주체: 보안 ID: S-1-5-21-2000478354-1123561945-725345543-500 계정 이름: vmadmin 계정 도메인: SAMPLECORP 로그인 ID: 0x1EBACD7E 대상 계정: 보안 ID: S-1-5-21-2000478354-1123561945-725345543-7605 계정 이름: SMP-WEB\$ 계정 도메인: SAMPLECORP
<b>원인:</b> 사용자 계정 활성화 <b>조치:</b> 활성화 주체 확인, 비인가 시 원복			
2026-05-06 14:06	계정 비활성화	4725	사용자 계정을 사용할 수 없습니다. 주체: 보안 ID: S-1-5-21-2000478354-1123561945-725345543-500 계정 이름: vmadmin 계정 도메인: SAMPLECORP 로그인 ID: 0x1EBACD7E 대상 계정: 보안 ID: S-1-5-21-2000478354-1123561945-725345543-7605 계정 이름: SMP-WEB\$ 계정 도메인: SAMPLECORP
<b>원인:</b> 사용자 계정 비활성화 <b>조치:</b> 비활성화 주체 및 사유 확인			
2026-05-06 14:06	관리자 암호 재설정	4724	계정 암호를 다시 설정하려고 했습니다. 주체: 보안 ID: S-1-5-21-2000478354-1123561945-725345543-500 계정 이름: vmadmin 계정 도메인: SAMPLECORP 로그인 ID: 0x1EBACD7E 대상 계정: 보안 ID: S-1-5-21-2000478354-1123561945-725345543-7605 계정 이름: SMP-WEB\$ 계정 도메인: SAMPLECORP
<b>원인:</b> 관리자에 의한 비밀번호 재설정 <b>조치:</b> 재설정 주체 및 대상 계정 확인			

▲ 제일 위로

#### 4. 수집 이력 (60일)

▲ 제일 위로

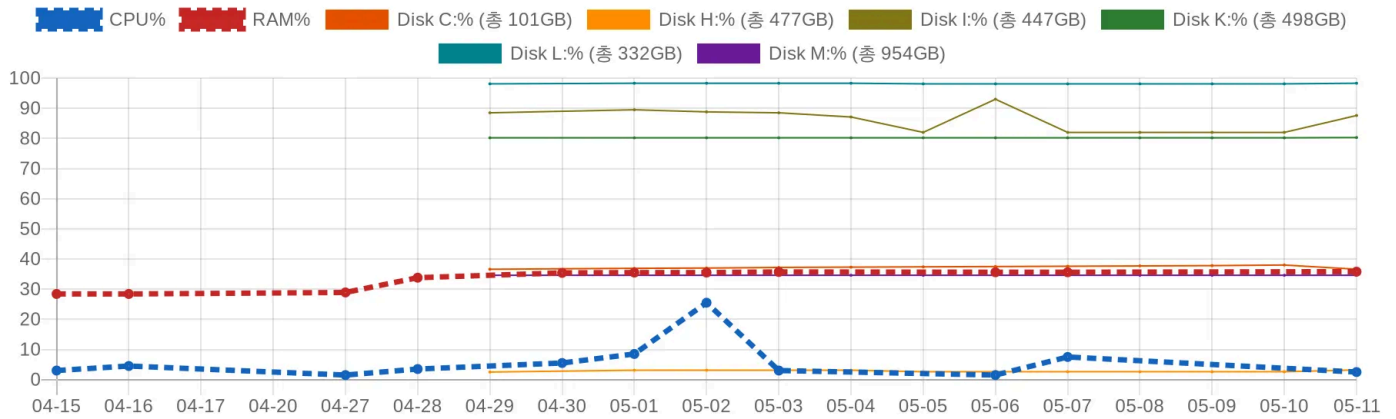
## Windows Monitor — 4. 수집 이력

샘플IDC

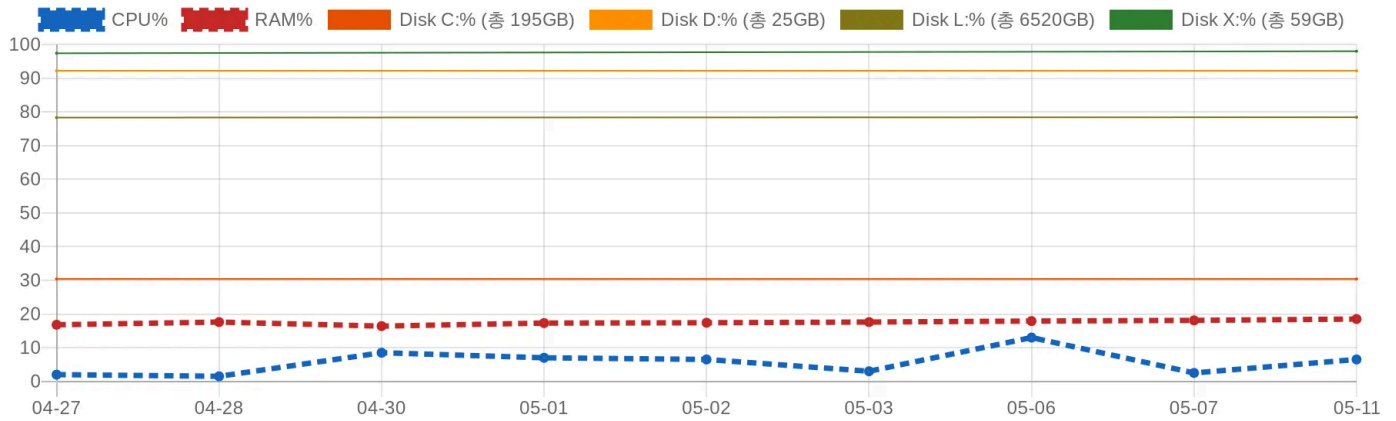
IT 운영팀 | 2026년 05월 11일 13:39

# 리소스 추이 (최근 60일)

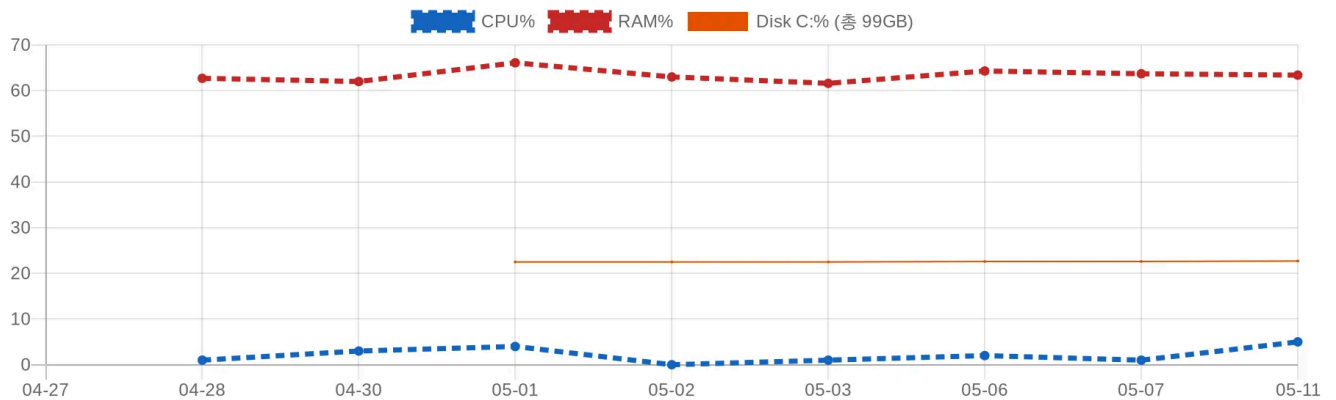
## SMP-PC 테스트 서버



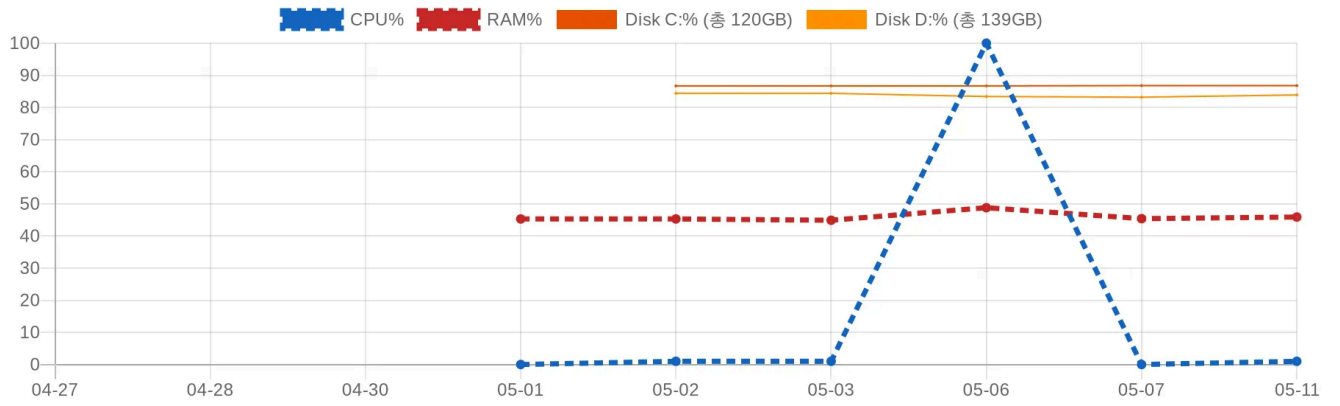
## VHOST-DR01 Hyper-V Host (DR) - 외부 점프서버



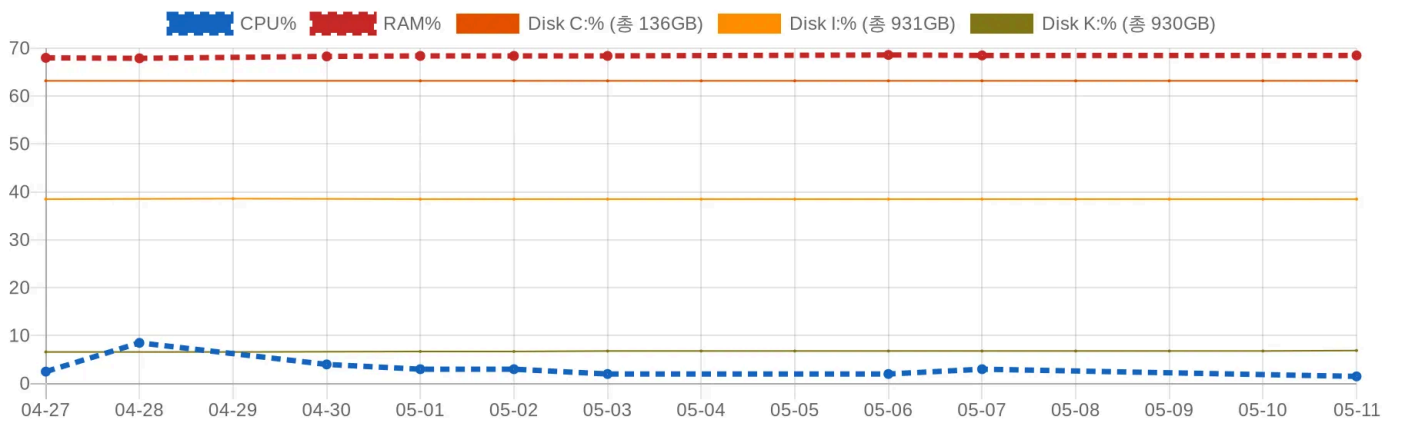
## SMP-DC02 Hyper-V Guest (SAMPLECORP 도메인)



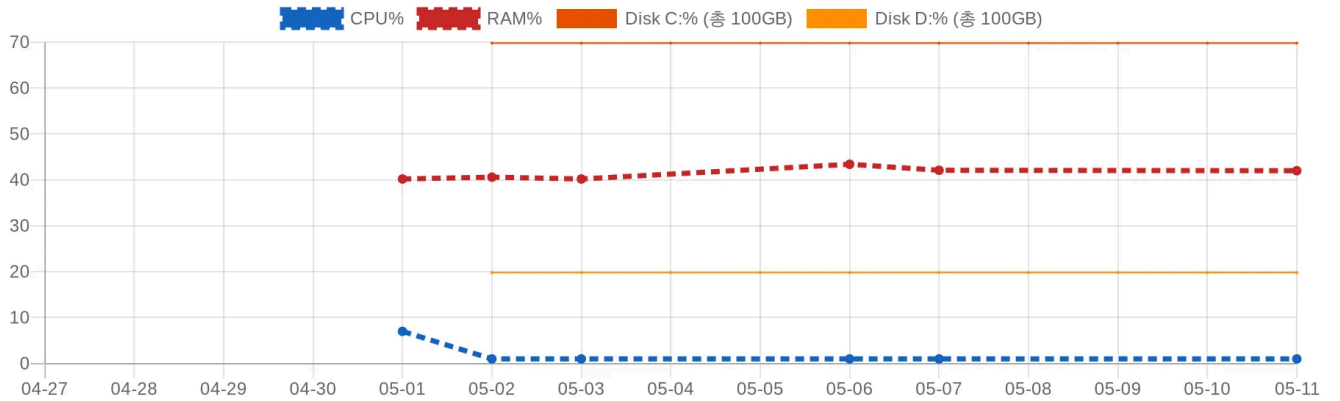
### CORP1-MAIL Hyper-V Guest (CORP1)



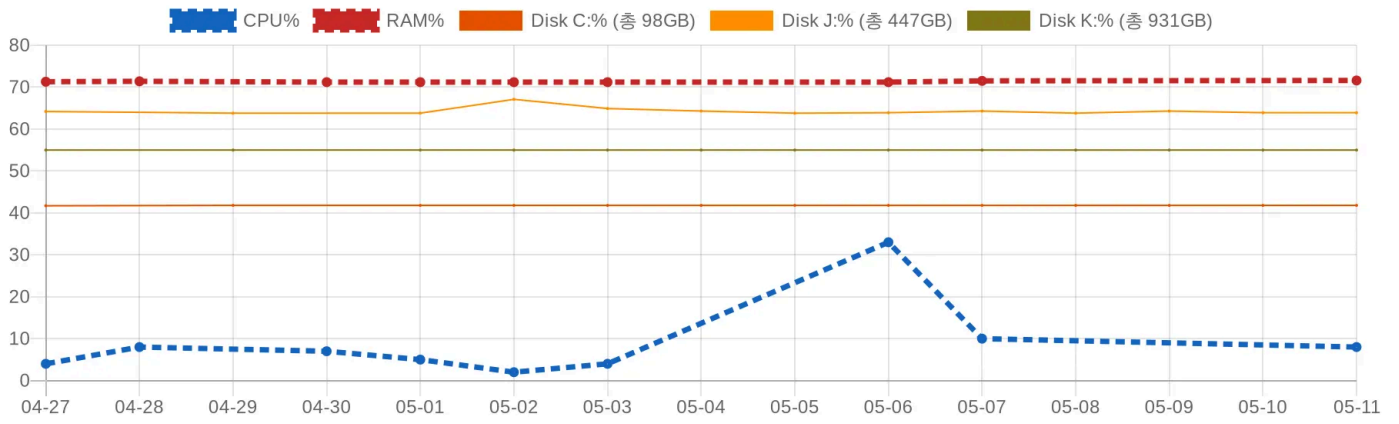
### VHOST-01 Hyper-V Host (IDC 내부)



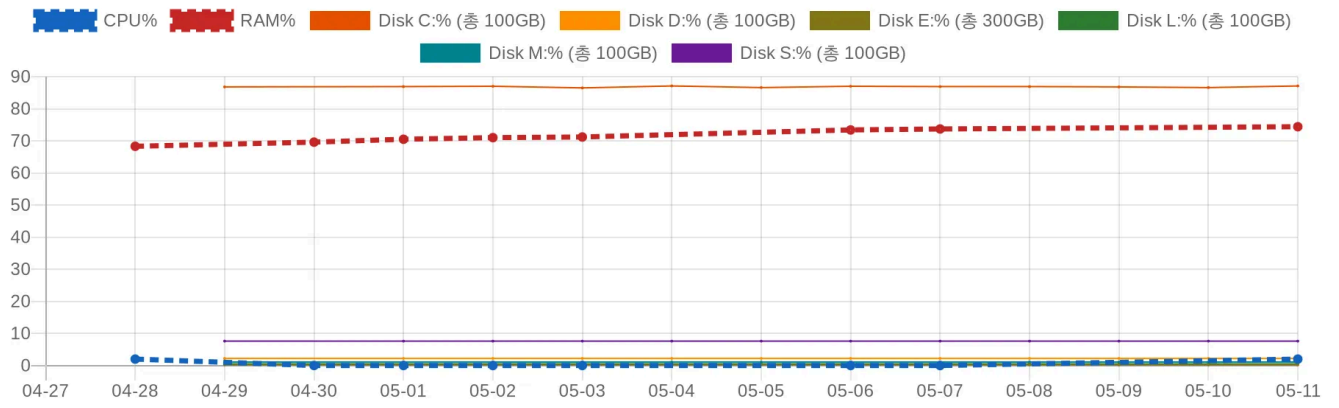
### CORP1-APP Hyper-V Guest (CORP1)



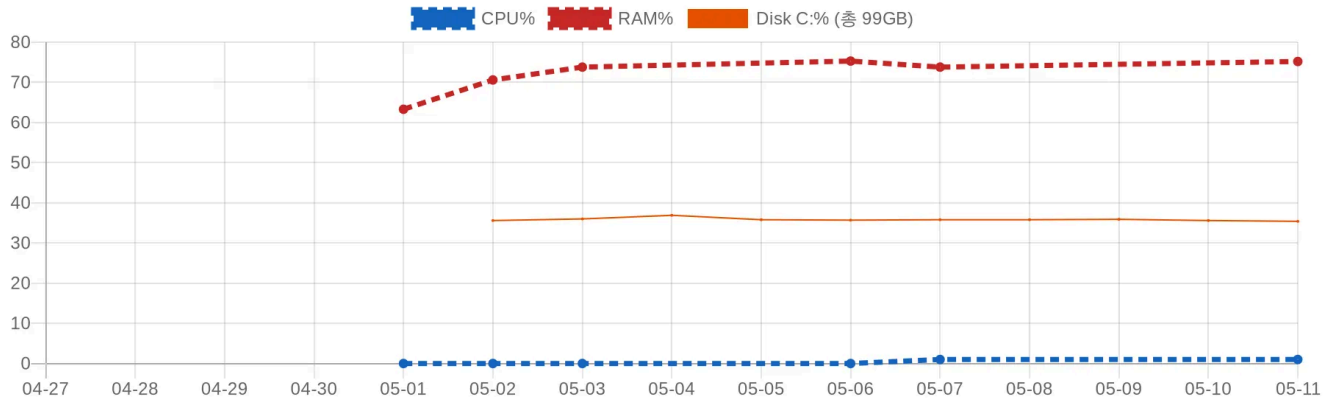
### VHOST-03 Hyper-V Host (IDC 내부)



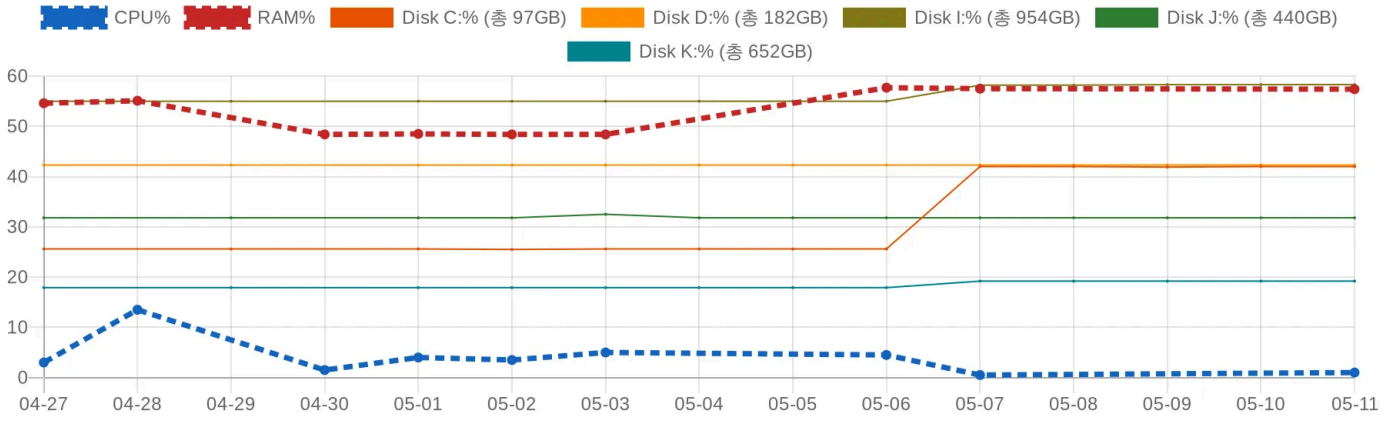
### SMP-SQL Hyper-V Guest (내부)



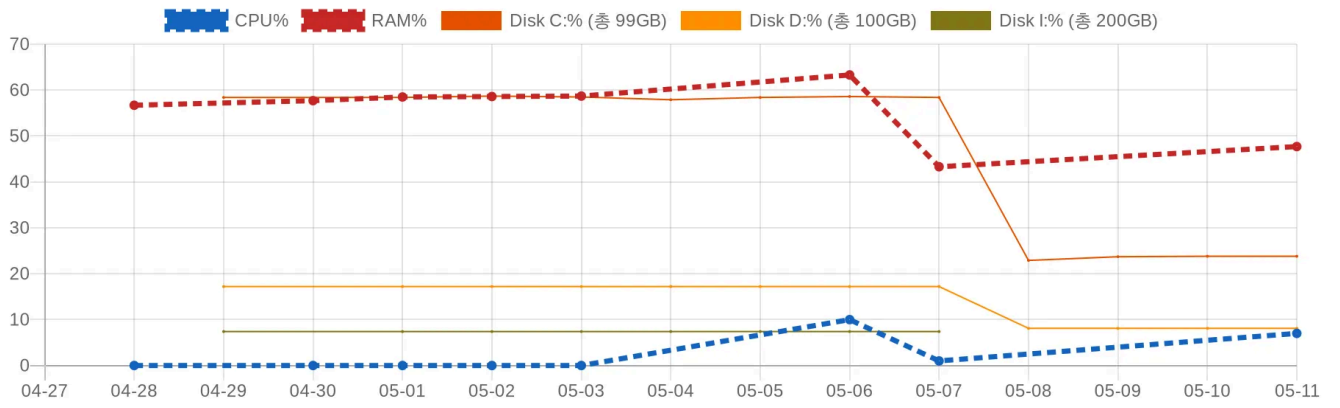
### REMOTE-A 샘플IDC 원격접속 서버



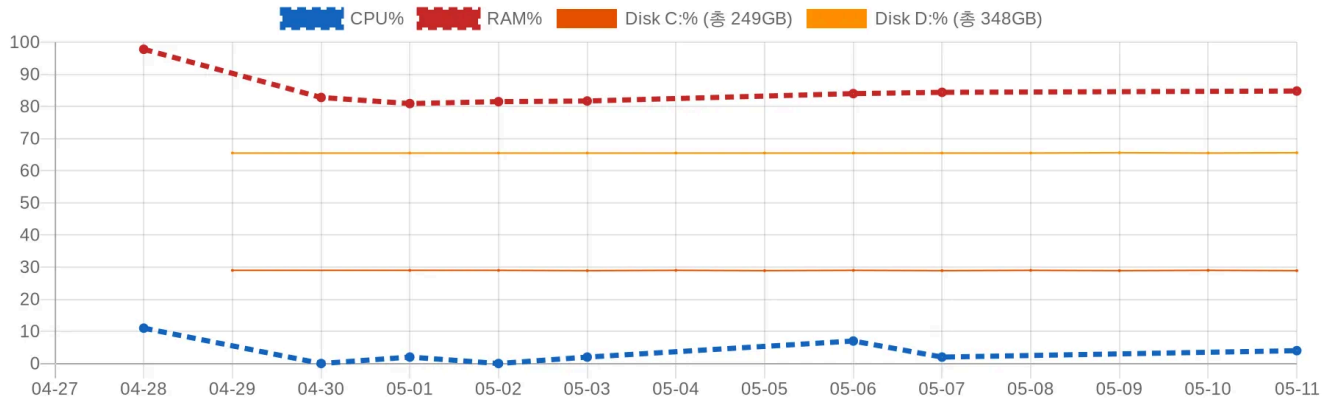
### VHOST-31 Hyper-V Host (IDC 내부)



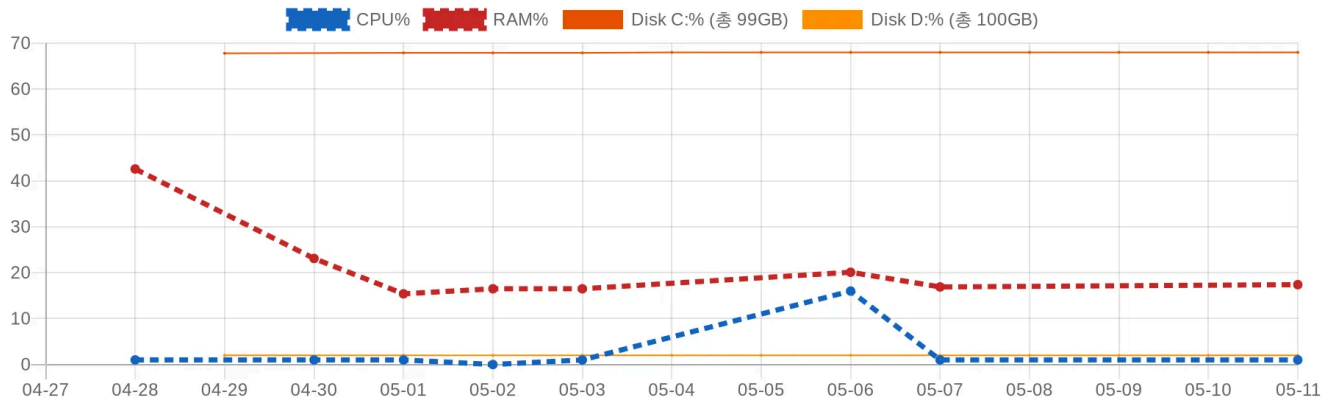
### SMP-WEB Hyper-V Guest



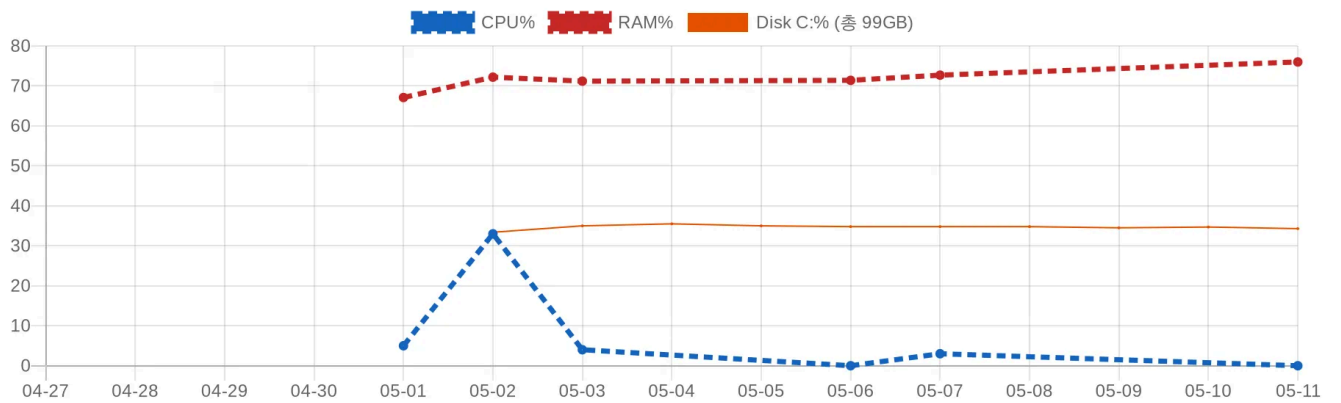
### SMP-EX02 Hyper-V Guest (mailhost)



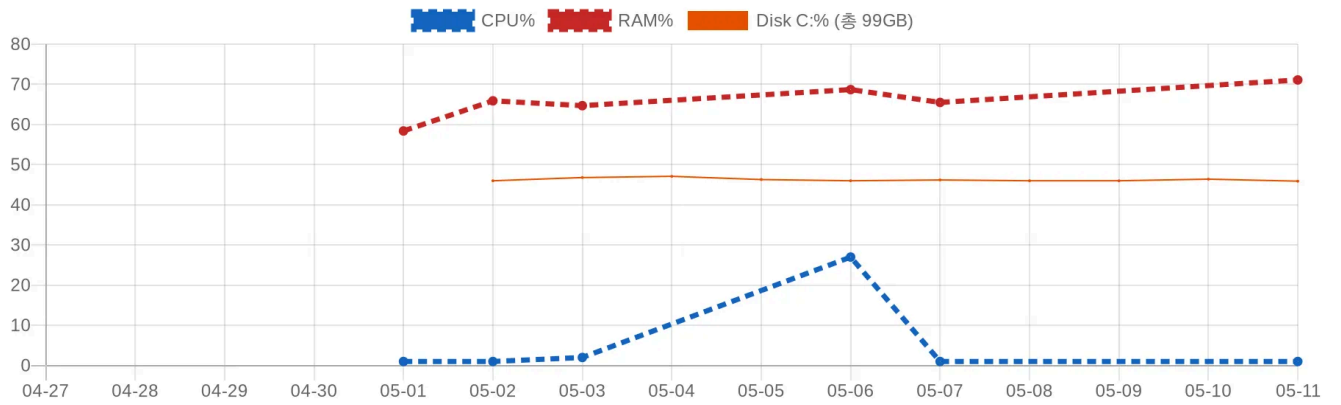
### SMP-SMTP Hyper-V Guest



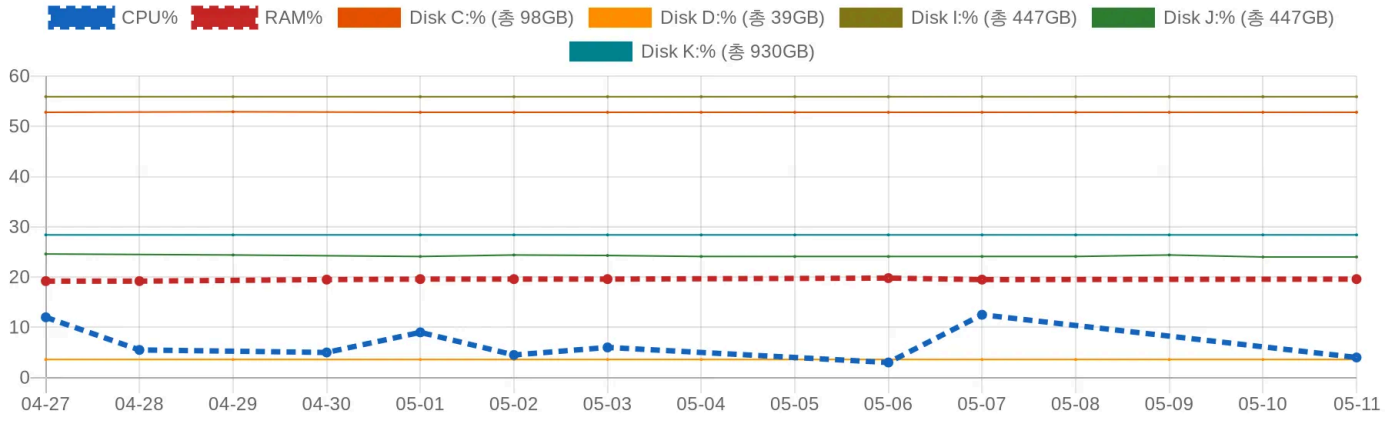
### REMOTE-B 샘플IDC 원격접속 서버



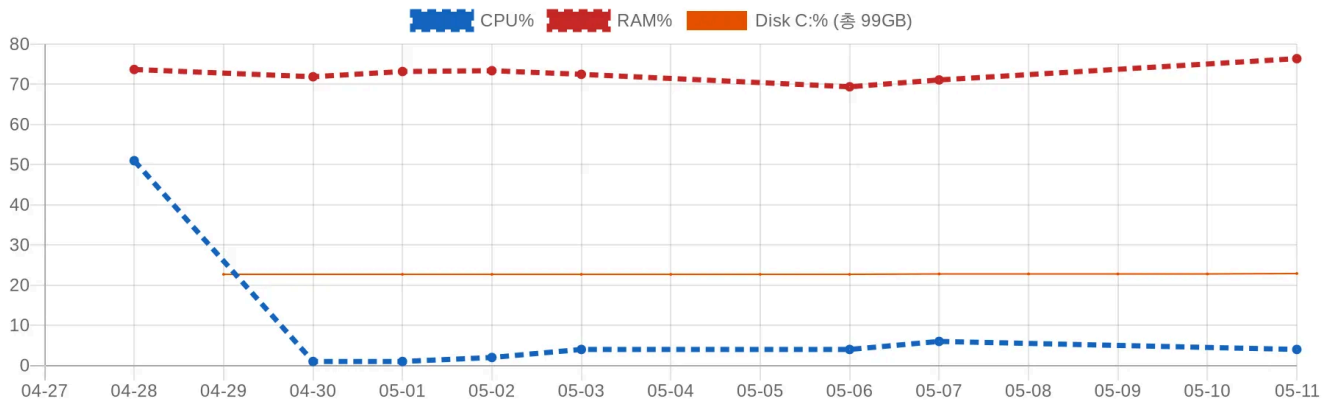
### REMOTE-C 샘플IDC 원격접속 서버



## VHOST-32 Hyper-V Host (IDC 내부)



## SMP-DC01 Hyper-V Guest (SAMPLECORP 도메인)



▲ 제일 위로

## 7. WinRM 보안

▲ 제일 위로

# Windows Monitor — 7. WinRM 보안

샘플IDC

IT 운영팀 | 2026년 05월 11일 13:39

## WinRM 5985 방화벽 룰

### SMP-PC 10.0.20.50 — 활성 10개 (허용 0 / 차단 0)

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
Hyper-V - WMI(Async-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V - WMI(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V 관리 클라이언트 - WMI (Async-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V 관리 클라이언트 - WMI (TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
Samsung UPD Service2	허용	공용	UDP/모두	모두
Samsung UPD Service2	허용	공용	TCP/모두	모두
Windows 원격 관리(HTTP-In)	허용	도메인,개인	TCP/5985	모두
Windows 원격 관리(HTTP-In)	허용	공용	TCP/5985	LocalSubnet
WinRM HTTP (Claude Monitor)	허용	도메인,개인,공용	TCP/5985	모두
원격 데스크톱 - 새도(TCP-In)	허용	도메인,개인	TCP/모두	모두

### VHOST-DR01 100.100.180.190 — 활성 10개 (허용 0 / 차단 0)

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
Anyadmin-sup	허용	공용	TCP/모두	모두
Anyadmin-sup	허용	공용	UDP/모두	모두
Hyper-V - WMI(Async-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V - WMI(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V 관리 클라이언트 - WMI (Async-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V 관리 클라이언트 - WMI (TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
USB Redirector Service	허용	도메인,개인,공용	TCP/모두	모두
Windows 원격 관리(HTTP-In)	허용	공용	TCP/5985	모두
Windows 원격 관리(HTTP-In)	허용	도메인,개인	TCP/5985	모두
원격 데스크톱 - 새도(TCP-In)	허용	도메인,개인	TCP/모두	모두

### SMP-DC02 100.100.180.187 — 활성 10개 (허용 0 / 차단 0)

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
AllJoyn 라우터(UDP-In)	허용	도메인,개인	UDP/모두	모두
Windows 원격 관리(HTTP-In)	허용	공용	TCP/5985	모두
Windows 원격 관리(HTTP-In)	허용	도메인,개인	TCP/5985	모두
WinRM-5985	허용	도메인,개인	TCP/5985	모두
WMI(Windows Management Instrumentation)(ASync-In)	허용	도메인,개인,공용	TCP/모두	모두
WMI(Windows Management Instrumentation)(WMI-In)	허용	도메인,개인,공용	TCP/모두	모두
원격 데스크톱 - 새도(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	개인	UDP/모두	LocalSubnet
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	도메인	UDP/모두	모두
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	공용	UDP/모두	모두

**CORP1-MAIL 200.200.227.205 — 활성 9개 (허용 0 / 차단 0)**

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
Deny-All	차단	도메인,개인,공용	TCP/모두	185.217.0.0/16
Email Login Failed_IP Deny	차단	도메인,개인,공용	TCP/모두	103.207.36.70/32
Windows 원격 관리(HTTP-In)	허용	도메인,개인	TCP/5985	모두
Windows 원격 관리(HTTP-In)	허용	공용	TCP/5985	모두
WinRM-5985	허용	도메인,개인,공용	TCP/5985	모두
WMI(Windows Management Instrumentation)(ASync-In)	허용	도메인,개인,공용	TCP/모두	모두
WMI(Windows Management Instrumentation)(WMI-In)	허용	도메인,개인,공용	TCP/모두	모두
원격 데스크톱 - 새도(TCP-In)	허용	공용	TCP/모두	모두
원격 데스크톱 - 새도(TCP-In)	허용	도메인,개인	TCP/모두	모두

**VHOST-01 10.0.10.11 — 활성 7개 (허용 0 / 차단 0)**

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
Hyper-V - WMI(ASync-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V - WMI(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V 관리 클라이언트 - WMI (ASync-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V 관리 클라이언트 - WMI (TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
Windows 원격 관리(HTTP-In)	허용	공용	TCP/5985	LocalSubnet
Windows 원격 관리(HTTP-In)	허용	도메인,개인	TCP/5985	모두
원격 데스크톱 - 새도(TCP-In)	허용	도메인,개인	TCP/모두	모두

**CORP1-APP 200.200.227.204 — 활성 24개 (허용 0 / 차단 0)**

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
Douzone.Wehago.BusinessHost	허용	개인	UDP/모두	모두
Douzone.Wehago.BusinessHost	차단	개인	TCP/모두	모두
Duzon SDB Server	허용	개인	UDP/모두	모두
Duzon SDB Server	허용	개인	TCP/모두	모두
DuzonDigital DB Server	허용	개인	TCP/모두	모두
DuzonDigital DB Server	허용	개인	TCP/모두	모두
DuzonDigital DB Server	허용	개인	UDP/모두	모두
DuzonDigital DB Server	허용	개인	UDP/모두	모두
iProxy	허용	개인	TCP/모두	모두
iProxy	허용	개인	UDP/모두	모두
Java(TM) Platform SE binary	허용	개인	TCP/모두	모두
Java(TM) Platform SE binary	허용	개인	UDP/모두	모두
NeoiPlusUpdaterClient	허용	개인	TCP/모두	모두
NeoiPlusUpdaterClient	허용	개인	UDP/모두	모두
NeoRSService	허용	공용	UDP/모두	모두
NeoRSService	허용	공용	TCP/모두	모두
USB Redirector Client Service	허용	도메인,개인,공용	TCP/모두	모두
Windows 원격 관리(HTTP-In)	허용	공용	TCP/5985	모두
Windows 원격 관리(HTTP-In)	허용	도메인,개인	TCP/5985	모두
WinRM-5985	허용	도메인,개인	TCP/5985	모두
네오플러스 메인 프로그램	허용	개인	UDP/모두	모두
네오플러스 메인 프로그램	허용	개인	TCP/모두	모두
원격 데스크톱 - 새도(TCP-In)	허용	도메인,개인	TCP/모두	모두
원격 데스크톱 - 새도(TCP-In)	허용	공용	TCP/모두	모두

**VHOST-03 10.0.10.13 — 활성 15개 (허용 0 / 차단 0)**

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
Anyadmin-sup	허용	공용	TCP/모두	모두
Anyadmin-sup	허용	공용	UDP/모두	모두
Hyper-V - WMI(Async-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V - WMI(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V 관리 클라이언트 - WMI (Async-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V 관리 클라이언트 - WMI (TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
Teamviewer Remote Control Application	허용	공용	TCP/모두	모두
Teamviewer Remote Control Application	허용	공용	UDP/모두	모두
Teamviewer Remote Control Service	허용	공용	TCP/모두	모두
Teamviewer Remote Control Service	허용	공용	UDP/모두	모두
Windows 원격 관리(HTTP-In)	허용	공용	TCP/5985	LocalSubnet
Windows 원격 관리(HTTP-In)	허용	도메인,개인	TCP/5985	모두
WMI(Windows Management Instrumentation)(ASync-In)	허용	도메인,개인,공용	TCP/모두	모두
WMI(Windows Management Instrumentation)(WMI-In)	허용	도메인,개인,공용	TCP/모두	모두
원격 데스크톱 - 새도(TCP-In)	허용	도메인,개인	TCP/모두	모두

**SMP-SQL 10.0.30.250 — 활성 2개 (허용 0 / 차단 0)**

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
Windows 원격 관리(HTTP-In)	허용	도메인,개인,공용	TCP/5985	모두
WinRM-5985	허용	도메인,개인,공용	TCP/5985	모두

REMOTE-A 10.0.30.55 — 활성 43개 (허용 0 / 차단 0)

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
AllJoyn 라우터(UDP-In)	허용	도메인,개인	UDP/모두	모두
Anyadmin-sup	허용	공용	TCP/모두	모두
Anyadmin-sup	허용	공용	UDP/모두	모두
AXGATE VPN Client	허용	공용	UDP/모두	모두
AXGATE VPN Client	허용	공용	TCP/모두	모두
DBSAFER AGENT	허용	공용	UDP/모두	모두
DBSAFER AGENT	허용	공용	TCP/모두	모두
DBSAFER AGENT	허용	개인	TCP/모두	모두
DBSAFER AGENT	허용	개인	UDP/모두	모두
Internet Explorer	차단	공용	TCP/모두	모두
Internet Explorer	허용	개인	TCP/모두	모두
Internet Explorer	허용	개인	UDP/모두	모두
Internet Explorer	차단	공용	UDP/모두	모두
Skype	허용	도메인,개인,공용	TCP/모두	모두
Skype	허용	도메인,개인,공용	UDP/모두	모두
Skype	허용	도메인,개인,공용	TCP/모두	모두
Skype	허용	도메인,개인,공용	TCP/모두	모두
Skype	허용	도메인,개인,공용	UDP/모두	모두
Skype	허용	도메인,개인,공용	UDP/모두	모두
Skype for Business	허용	공용	UDP/모두	모두
Skype for Business	허용	공용	TCP/모두	모두
Skype for Business	허용	개인	UDP/모두	모두
Skype for Business	허용	개인	TCP/모두	모두
Skype for Business Ucmapi	허용	공용	TCP/모두	모두
Skype for Business Ucmapi	허용	공용	UDP/모두	모두
Skype for Business Ucmapi	허용	개인	TCP/모두	모두
Skype for Business Ucmapi	허용	개인	UDP/모두	모두
TCP를 통한 근접 공유(TCP 공유-내부)	허용	도메인,개인,공용	TCP/모두	모두
WFD 드라이버 전용(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
WFD 드라이버 전용(UDP-In)	허용	도메인,개인,공용	UDP/모두	모두
Windows 원격 관리(HTTP-In)	허용	공용	TCP/5985	모두
Windows 원격 관리(HTTP-In)	허용	도메인,개인	TCP/5985	모두
WinRM-5985	허용	도메인,개인	TCP/5985	모두
무선 디스플레이(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
연결된 장치 플랫폼 - Wi-Fi Direct 전송(TCP-In)	허용	공용	TCP/모두	모두
연결된 장치 플랫폼(TCP-In)	허용	도메인,개인	TCP/모두	모두
연결된 장치 플랫폼(UDP-In)	허용	도메인,개인	UDP/모두	모두

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
원격 데스크톱 - 새도(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
원격 지원(RA Server TCP-In)	허용	도메인	TCP/모두	모두
원격 지원(TCP-In)	허용	도메인,개인	TCP/모두	모두
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	도메인	UDP/모두	모두
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	공용	UDP/모두	모두
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	개인	UDP/모두	LocalSubnet

### VHOST-31 10.0.10.31 — 활성 11개 (허용 0 / 차단 0)

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
D:\Install\hpsum751\hpsum\wx64\hpsum_service_x64.exe	허용	공용	TCP/모두	모두
D:\Install\hpsum751\hpsum\wx64\hpsum_service_x64.exe	허용	공용	UDP/모두	모두
Hyper-V - WMI(Async-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V - WMI(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V 관리 클라이언트 - WMI (Async-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V 관리 클라이언트 - WMI (TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
Windows 원격 관리(HTTP-In)	허용	공용	TCP/5985	LocalSubnet
Windows 원격 관리(HTTP-In)	허용	도메인,개인	TCP/5985	모두
WMI(Windows Management Instrumentation)(ASync-In)	허용	도메인,개인,공용	TCP/모두	모두
WMI(Windows Management Instrumentation)(WMI-In)	허용	도메인,개인,공용	TCP/모두	모두
원격 데스크톱 - 새도(TCP-In)	허용	도메인,개인	TCP/모두	모두

### SMP-WEB 100.100.180.184 — 활성 9개 (허용 0 / 차단 0)

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
AllJoyn 라우터(UDP-In)	허용	도메인,개인	UDP/모두	모두
Windows 원격 관리(HTTP-In)	허용	도메인,개인	TCP/5985	모두
Windows 원격 관리(HTTP-In)	허용	공용	TCP/5985	모두
WMI(Windows Management Instrumentation)(ASync-In)	허용	도메인,개인,공용	TCP/모두	모두
WMI(Windows Management Instrumentation)(WMI-In)	허용	도메인,개인,공용	TCP/모두	모두
원격 데스크톱 - 새도(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	개인	UDP/모두	LocalSubnet
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	도메인	UDP/모두	모두
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	공용	UDP/모두	모두

**SMP-EX02 100.100.180.180 — 활성 5개 (허용 0 / 차단 0)**

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
Deny-All	차단	도메인, 개인, 공용	TCP / 1-65535	12.150.45.0/24,23.94.169.0/24,40.100.0.0/16,45.66.230.0/24,45.129.14.0/24,45.142.120.0/24,45.148.10.0/24,46.148.40.0/24,51.210.60.0/24,77.0.0.0/8,80.94.95.0/24,88.200.167.0/24,89.248.174.3/32,91.200.12.0/24,93.174.93.166/32,103.167.40.0/24,103.231.139.0/24,121.202.203.0/24,141.98.10.0/24,141.98.11.0/24,145.249.105.210/32,145.249.107.135/32,157.52.179.0/24,158.94.209.0/24,172.93.52.0/24,181.214.206.189/32,181.217.206.0/24,185.93.3.0/24,185.246.255.0/24,191.96.249.177/32,212.70.149.0/24,213.32.253.0/24,213.209.157.0/24,222.119.124.0/24
Windows 원격 관리 (HTTP-In)	허용	도메인, 개인, 공용	TCP / 5985	모두
WinRM-5985	허용	도메인, 개인, 공용	TCP / 5985	모두
WMI(Windows Management Instrumentation) (ASync-In)	허용	도메인, 개인, 공용	TCP / 모두	모두
WMI(Windows Management Instrumentation) (WMI-In)	허용	도메인, 개인, 공용	TCP / 모두	모두

**SMP-SMTP 200.200.227.226 — 활성 5개 (허용 0 / 차단 0)**

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
Deny-all	차단	도메인, 개인, 공용	TCP / 1-65534	45.142.0.0/16
Windows 원격 관리(HTTP-In)	허용	도메인, 개인	TCP / 5985	모두
Windows 원격 관리(HTTP-In)	허용	공용	TCP / 5985	모두
WinRM-5985	허용	도메인, 개인	TCP / 5985	모두
원격 데스크톱 - 새도(TCP-In)	허용	도메인, 개인	TCP / 모두	모두

REMOTE-B 10.0.30.56 — 활성 47개 (허용 0 / 차단 0)

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
AllJoyn 라우터(UDP-In)	허용	도메인,개인	UDP/모두	모두
AXGATE VPN Client	허용	공용	UDP/모두	모두
AXGATE VPN Client	허용	개인	UDP/모두	모두
AXGATE VPN Client	허용	개인	TCP/모두	모두
AXGATE VPN Client	허용	공용	TCP/모두	모두
DBSAFER AGENT	허용	개인,공용	UDP/모두	모두
DBSAFER AGENT	허용	공용	UDP/모두	모두
DBSAFER AGENT	허용	개인	UDP/모두	모두
DBSAFER AGENT	허용	개인	TCP/모두	모두
DBSAFER AGENT	허용	개인	UDP/모두	모두
DBSAFER AGENT	허용	개인	TCP/모두	모두
DBSAFER AGENT	허용	개인,공용	TCP/모두	모두
DBSAFER AGENT	허용	공용	TCP/모두	모두
DBSAFER AGENT	허용	공용	TCP/모두	모두
DBSAFER AGENT	허용	공용	UDP/모두	모두
DBSAFER AGENT	허용	공용	TCP/모두	모두
DBSAFER AGENT	허용	공용	UDP/모두	모두
ezHelp Server for Windows	허용	도메인,개인,공용	TCP/모두	모두
ezHelp Server Remote File Module for Windows	허용	도메인,개인,공용	TCP/모두	모두
ezHelp Server Sound Module for Windows	허용	도메인,개인,공용	TCP/모두	모두
Internet Explorer	차단	개인	UDP/모두	모두
Internet Explorer	차단	개인	TCP/모두	모두
Internet Explorer	허용	공용	TCP/모두	모두
Internet Explorer	허용	공용	UDP/모두	모두
ms-resource:AppTitle	허용	도메인,개인,공용	TCP/모두	모두
Skype for Business	허용	개인	TCP/모두	모두
Skype for Business	허용	개인	UDP/모두	모두
Skype for Business Ucmapi	허용	개인	UDP/모두	모두
Skype for Business Ucmapi	허용	개인	TCP/모두	모두
TCP를 통한 근접 공유(TCP 공유-내부)	허용	도메인,개인,공용	TCP/모두	모두
WFD 드라이버 전용(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
WFD 드라이버 전용(UDP-In)	허용	도메인,개인,공용	UDP/모두	모두
Windows 원격 관리(HTTP-In)	허용	도메인,개인	TCP/5985	모두
Windows 원격 관리(HTTP-In)	허용	공용	TCP/5985	모두
WinNGS Listen	허용	공용	TCP/모두	모두
WinNGS Listen	허용	공용	UDP/모두	모두
WinRM-5985	허용	도메인,개인	TCP/5985	모두

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
무선 디스플레이(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
연결된 장치 플랫폼 - Wi-Fi Direct 전송(TCP-In)	허용	공용	TCP/모두	모두
연결된 장치 플랫폼(TCP-In)	허용	도메인,개인	TCP/모두	모두
연결된 장치 플랫폼(UDP-In)	허용	도메인,개인	UDP/모두	모두
원격 데스크톱 - 새도(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
원격 지원(RA Server TCP-In)	허용	도메인	TCP/모두	모두
원격 지원(TCP-In)	허용	도메인,개인	TCP/모두	모두
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	공용	UDP/모두	모두
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	개인	UDP/모두	LocalSubnet
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	도메인	UDP/모두	모두

REMOTE-C 10.0.30.57 — 활성 51개 (허용 0 / 차단 0)

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
AllJoyn 라우터(UDP-In)	허용	도메인,개인	UDP/모두	모두
Anyadmin-sup	허용	공용	TCP/모두	모두
Anyadmin-sup	허용	공용	UDP/모두	모두
AXGATE VPN Client	허용	개인	TCP/모두	모두
AXGATE VPN Client	허용	개인	UDP/모두	모두
DBSAFER AGENT	허용	개인	TCP/모두	모두
DBSAFER AGENT	허용	개인	UDP/모두	모두
DBSAFER AGENT	허용	공용	UDP/모두	모두
DBSAFER AGENT	허용	공용	TCP/모두	모두
DBSAFER AGENT	허용	공용	TCP/모두	모두
DBSAFER AGENT	허용	개인	UDP/모두	모두
DBSAFER AGENT	허용	개인	TCP/모두	모두
DBSAFER AGENT	허용	개인,공용	UDP/모두	모두
DBSAFER AGENT	허용	개인,공용	TCP/모두	모두
DBSAFER AGENT	허용	공용	UDP/모두	모두
HelpU	허용	공용	TCP/모두	모두
HelpU	허용	공용	UDP/모두	모두
HIWARE PSM Client Proxy v6.0	허용	공용	UDP/모두	모두
HIWARE PSM Client Proxy v6.0	허용	공용	TCP/모두	모두
HIWARE PSM Client v6.0	허용	공용	UDP/모두	모두
HIWARE PSM Client v6.0	허용	공용	TCP/모두	모두
Internet Explorer	차단	개인	TCP/모두	모두
Internet Explorer	차단	개인	UDP/모두	모두
Skype	허용	도메인,개인,공용	UDP/모두	모두
Skype	허용	도메인,개인,공용	TCP/모두	모두
Skype	허용	도메인,개인,공용	TCP/모두	모두
Skype	허용	도메인,개인,공용	UDP/모두	모두
Skype	허용	도메인,개인,공용	UDP/모두	모두
Skype	허용	도메인,개인,공용	UDP/모두	모두
Skype	허용	도메인,개인,공용	TCP/모두	모두
Skype	허용	도메인,개인,공용	TCP/모두	모두
Skype for Business	허용	개인	TCP/모두	모두
Skype for Business	허용	개인	UDP/모두	모두
Skype for Business Ucmapi	허용	개인	UDP/모두	모두
Skype for Business Ucmapi	허용	개인	TCP/모두	모두
TCP를 통한 근접 공유(TCP 공유-내부)	허용	도메인,개인,공용	TCP/모두	모두
Teredo용 네트워크 검색(SSDP-In)	허용	공용	UDP/모두	모두

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
Teredo용 네트워크 검색(UPnP-In)	허용	공용	TCP/모두	모두
WFD 드라이버 전용(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
WFD 드라이버 전용(UDP-In)	허용	도메인,개인,공용	UDP/모두	모두
WinRM-5985	허용	도메인,개인	TCP/5985	모두
무선 디스플레이(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
연결된 장치 플랫폼 - Wi-Fi Direct 전송(TCP-In)	허용	공용	TCP/모두	모두
연결된 장치 플랫폼(TCP-In)	허용	도메인,개인	TCP/모두	모두
연결된 장치 플랫폼(UDP-In)	허용	도메인,개인	UDP/모두	모두
원격 데스크톱 - 새도(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
원격 지원(RA Server TCP-In)	허용	도메인	TCP/모두	모두
원격 지원(TCP-In)	허용	도메인,개인	TCP/모두	모두
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	도메인	UDP/모두	모두
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	공용	UDP/모두	모두
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	개인	UDP/모두	LocalSubnet

#### VHOST-32 10.0.10.32 — 활성 7개 (허용 0 / 차단 0)

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
Hyper-V - WMI(Async-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V - WMI(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V 관리 클라이언트 - WMI (Async-In)	허용	도메인,개인,공용	TCP/모두	모두
Hyper-V 관리 클라이언트 - WMI (TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
Windows 원격 관리(HTTP-In)	허용	공용	TCP/5985	LocalSubnet
Windows 원격 관리(HTTP-In)	허용	도메인,개인	TCP/5985	모두
원격 데스크톱 - 새도(TCP-In)	허용	도메인,개인	TCP/모두	모두

#### SMP-DC01 100.100.180.182 — 활성 10개 (허용 0 / 차단 0)

룰 이름	동작	프로필	프로토콜/포트	허용 영역 (RemoteAddress)
AllJoyn 라우터(UDP-In)	허용	도메인,개인	UDP/모두	모두
Windows 원격 관리(HTTP-In)	허용	공용	TCP/5985	LocalSubnet
Windows 원격 관리(HTTP-In)	허용	도메인,개인	TCP/5985	모두
WinRM-5985	허용	도메인,개인	TCP/5985	모두
WMI(Windows Management Instrumentation)(ASync-In)	허용	도메인,개인,공용	TCP/모두	모두
WMI(Windows Management Instrumentation)(WMI-In)	허용	도메인,개인,공용	TCP/모두	모두
원격 데스크톱 - 새도(TCP-In)	허용	도메인,개인,공용	TCP/모두	모두
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	개인	UDP/모두	LocalSubnet
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	도메인	UDP/모두	모두
장치로 캐스트 스트리밍 서버(RTCP-Streaming-In)	허용	공용	UDP/모두	모두