

NetScaler SDX 13.1

Contents

はじめに	17
リリースノート	18
Management Serviceユーザーインターフェイスの利用を開始する	19
Management Serviceユーザーインターフェイスにログオンする	19
初期セットアップウィザード	20
SDXアプライアンス上でのインスタンスのプロビジョニング	21
コンソールアクセス	22
Management Serviceの統計	22
Management ServiceおよびNetScalerインスタンスへのシングルサインオン	22
ホームページの管理	23
ポート	24
データガバナンス	26
NetScaler Console service connectとは何ですか?	26
NetScaler Console serviceとは何ですか?	27
NetScaler Consoleサービスコネクトはどのように有効になりますか?	27
NetScaler Consoleサービスコネクトを使用してどのようなデータが取得されますか?	27
データはどのように使用されますか?	28
収集されたデータはどのくらいの期間保持されますか?	28
データの保存場所と安全性?	28
NetScaler Console サービス接続を無効にする方法?	28
NetScaler SDXアプライアンス向けConsole Advisory Connectの概要	29
Console Advisory ConnectはNetScaler Consoleサービスをどのようにサポートしますか?	30
Console Advisory ConnectはどのバージョンのNetScalerでサポートされていますか?	30
Console Advisory Connectを有効にする方法?	30
Console Advisory Connectを有効化および無効化する方法?	31
CLIの使用	31

GUIの使用	31
NITRO API の使用	32
NetScaler Console 組み込みエージェントの動作	32
参照	32
シングルバンドルアップグレード	33
注意事項	33
アプライアンス全体を13.1にアップグレードする	34
サポートされているアップグレードパス	35
関連情報	35
NetScalerインスタンスのアップグレード	36
ソフトウェアイメージをアップロードするには	36
ビルドファイルをダウンロードしてバックアップを作成するには	37
XVAファイルをアップロードするには	37
XVAファイルをダウンロードしてバックアップを作成するには	37
NetScaler VPXインスタンスのアップグレード	37
VPXインスタンスをアップグレードするには	38
関連情報	38
SDXアプライアンスの管理と監視	39
SDXアプライアンスのネットワーク構成を変更する	39
デフォルトユーザーアカウントのパスワードを変更する	39
アプライアンスのタイムゾーンを変更する	39
アプライアンスのホスト名を変更する	40
VLANフィルタリング	40
クロック同期を構成する	40
NTP同期を有効にするには	41
認証オプションを変更するには	41
SDXアプライアンスのプロパティを表示する	42
アプライアンスのスループットをリアルタイムで表示する	43

CPUとメモリの使用状況をリアルタイムで表示する	43
すべてのコアのCPU使用率を表示する	44
SDXアプライアンスにSSL証明書をインストールする	44
Management ServiceでSSL証明書を表示する	44
NetScalerインスタンスのSSL証明書とキー	45
システム設定を変更する	45
アプライアンスを再起動する	45
アプライアンスをシャットダウンする	45
SDX 管理ドメイン	46
サブドメインへのリソース割り当ての例	46
ユーザーをドメインに割り当てる	47
SDX 22000 プラットフォームでのRAIDディスク割り当ての管理	48
ドライブのプロパティと操作を表示する	48
論理ドライブ	48
新しい論理ドライブを作成するには	49
物理ドライブ	49
ストレージリポジトリ	50
SDXライセンスの概要	52
ライセンスアクティベーションサービス	53
SDXアプライアンスでのライセンス管理	53
前提条件	54
Management Service を使用したライセンスの割り当て	54
ライセンスを割り当てるには	54
ライセンスアクティベーションサービス	56
LASのNetScalerバージョン互換性	57
前提条件	58
NetScaler GUIを使用してLASに移行する	58
ライセンスアクティベーションファイルの動作と有効期限	61

ライセンス契約の有効期限	61
LAS ライセンスワークフロー中に LAS に送信される情報	62
LAS に移行した NetScaler SDX (SVM) を監視するためのベストプラクティス	63
前提条件	63
LAS アクティベーションプロブの有効期限の監視	64
ライセンスエンタイトルメントの有効期限（契約の有効期限）の監視	65
SDXリソースビジュアライザー	66
インターフェースの管理	67
インターフェースを構成するには	67
インターフェイスのパラメータをデフォルト値にリセットするには	68
VPXインスタンス上の仮想インターフェイスと物理インターフェイスのマッピングを表示する	68
インターフェイスへのMACアドレスの割り当て	69
SDXアプライアンスの物理インターフェイスを無効または有効にする	70
SDXアプライアンスでのジャンボフレーム	71
ユースケース: ジャンボからジャンボへのセットアップ	71
ユースケース: 非ジャンボからジャンボへのセットアップ	75
ユースケース: 同じインターフェイスセット上でのジャンボフローと非ジャンボフローの共存	79
SDXアプライアンスでのSNMPの設定	86
SNMPトラップ宛先を追加するには	86
MIBファイルのダウンロード	87
MIBファイルをダウンロードするには	87
SNMPマネージャーコミュニティの追加	87
SNMPマネージャーを設定するには	88
SNMPv3クエリ用のSDXアプライアンスの構成	88
SNMPマネージャーの追加	89
SNMPビューの設定	89

ビューを設定するには	89
SNMPユーザーの構成	90
ユーザーを構成するには	90
SNMPアラームの設定	91
syslog通知を設定する	92
syslogサーバーを設定する	92
syslog パラメータを構成する	92
メール通知の構成	93
SMTPサーバーを構成するには	93
メールプロファイルを構成するには	93
SMS通知を構成する	93
SMSサーバーを構成する	93
SMSプロファイルを構成する	94
SDXアプライアンスで構成されたエンティティのリアルタイムステータスを監視および管理する	94
仮想サーバーのステータスを表示する	94
サービスのステータスを表示	95
サービスグループのステータスを表示する	96
サーバーのステータスを表示する	97
ポーリング間隔を構成する	98
NetScalerインスタンスで生成されたイベントの監視と管理	98
すべてのイベントを表示する	98
SDXアプライアンス上のNetScalerインスタンスに対するCall Homeサポート	102
システムヘルス監視	104
SDXアプライアンスのストレージリソースを監視する	104
SDXアプライアンスのハードウェアセンサーを監視する	105
SDXアプライアンスのインターフェースを監視する	106
システム通知設定の構成	107

システム通知設定を構成するには	107
マネジメントサービスから機能を有効/無効にする	107
GUI を使用して機能を有効または無効にするには	108
管理サービスを設定する	109
クライアントセッションを管理する	109
ポリシーを設定する	109
管理サービスを再起動する	111
管理サービスファイルを削除する	111
テクニカルサポート用のtarアーカイブを生成する	111
Management ServiceのCLIサポート	112
認証および承認設定の構成	113
ユーザーグループの追加	114
ユーザーグループを追加するには	114
ユーザーアカウントの設定	115
ユーザーアカウントを設定するには	115
ユーザーアカウントを削除するには	116
認証タイプを設定する	116
認証タイプを設定するには	116
基本認証を有効または無効にする	117
外部認証サーバーの構成	117
RADIUSサーバーの追加	117
RADIUSサーバーを追加するには	118
LDAP認証サーバーの追加	119
LDAPサーバーを追加するには	119
LDAPユーザーのSSH公開鍵認証のサポート	121
FQDN名前解決のためのプライマリDNSの追加	122
TACACSサーバーの追加	122
TACACSサーバーを追加するには	122

Management Serviceからリンクアグリゲーションを設定する	123
Management Serviceからのチャネルの構成	124
Management Serviceからチャネルを構成するには	124
アクセス制御リスト	126
使用ガイドライン	126
ACLを構成する方法	127
ACL機能を有効にする	127
ACLルールを作成する	127
ACLルールを有効にする	128
ACLルールのその他のアクション	128
ACLルールを無効にする	128
ACLルールを編集する	129
ACLルールを削除する	129
ACLルールの優先順位を振り直す	129
トラブルシューティング	130
NetScalerインスタンスのクラスターをセットアップする	130
留意事項	131
SDXアプライアンスでクラスターをセットアップする	132
あるSDXアプライアンスに存在するNetScalerインスタンスを、別のSDXアプライアンスで構成されたクラスターに追加する	134
クラスタリンクアグリゲーションの構成	135
管理サービスに安全にアクセスするためのSSL暗号の構成	138
制限事項	138
サポートされているSSL暗号	138
事前定義された暗号グループ	145
事前定義された暗号グループを表示する	146
カスタム暗号グループを作成する	147
既存のSSL暗号バインディングを表示する	147

HTTPSサービスに暗号をバインドする	147
SDXアプライアンスの構成データをバックアップおよび復元する	148
現在の構成をバックアップする	148
スケジュールされたバックアップ	149
バックアップポリシーの編集	149
バックアップファイルを外部バックアップサーバーに手動で転送する	149
バックアップファイルを外部バックアップサーバーに転送する	149
アプライアンスを復元する	150
バックアップファイルからアプライアンスを復元する	150
NetScalerインスタンスをリストアする	152
アプライアンスのリセットを実行する	153
アプライアンスの構成をリセットする	154
アプライアンスの設定をリセットする	154
アプライアンスを工場出荷時のバージョンにリセットする	154
アプライアンスを工場出荷時のバージョンにリセットする	155
アプライアンスをシングルバンドルイメージバージョンにリセットする	155
前提条件	156
アプライアンスを単一のバンドルイメージバージョンにリセットする	156
外部認証サーバーのカスケーディング	157
外部認証サーバーをカスケーディングする	157
ユーザーのロックを解除する	157
GUIを使用してユーザーのロックを解除する	158
CLIを使用してユーザーのロックを解除する	158
NetScalerインスタンスのプロビジョニング	159
管理者プロファイルの作成	160
管理者プロファイルの作成	161
NetScaler .xvaイメージをアップロードする	162
NetScaler .xva ファイルをアップロードするには	162

NetScaler .xva ファイルをダウンロードしてバックアップを作成するには	162
NetScaler インスタンスを追加する	163
ライセンスの割り当て	163
暗号化の割り当て	164
リソースの割り当て	164
SDX上のNetScaler VPXで追加の管理CPUを有効にするための推奨されるプラクティス	167
概要	168
追加の管理CPUを有効にするタイミング	169
インスタンス管理	170
ネットワーク設定	170
管理VLAN設定	172
NetScalerインスタンスの変更	172
VLANを特定の仮想インターフェイスに制限する	173
許可されたVLAN IDを指定するには	174
管理サービスからインスタンスのVLANを構成するには	174
暗号容量の管理	175
SDX アプライアンスの暗号容量を表示する	176
VPXインスタンスのプロビジョニング中に暗号容量を割り当てる	176
異なるSDXアプライアンスで利用可能なACUカウンターの最小値	176
暗号ハードウェアの健全性を表示	177
注意事項	178
ACUからPKEリソースへの変換テーブル	178
ACU から PKE へのリソース変換表の読み方	180
レガシーSSLチップからACUおよびSCUへの変換テーブル	181
サードパーティ製仮想マシンのプロビジョニング	182
SECUREMATRIX GSB	183
SECUREMATRIX GSBインスタンスをプロビジョニングする	183
SECUREMATRIXインスタンスをプロビジョニングするには	184

SECUREMATRIX GSBインスタンスを監視する	185
SECUREMATRIX GSBインスタンスを管理する	185
SECUREMATRIX GSBインスタンスのSDXツールファイルをアップグレードする	185
SECUREMATRIX GSBインスタンスのアップグレードとダウングレード	186
SECUREMATRIX GSBインスタンスのトラブルシューティング	187
トレンドマイクロ InterScan Web Security	188
ウェブセンス プロテクター	189
Websense Protector インスタンスをプロビジョニングする	189
XVAイメージをSDXアプライアンスにアップロードするには	190
Websense protectorインスタンスをプロビジョニングするには	190
Websense Protectorインスタンスを監視する	190
Websense Protectorインスタンスを管理する	191
Websense Protectorインスタンスを開始、停止、再起動、強制停止、または強制再起動するには	191
Websense ProtectorインスタンスのSDXツールファイルをアップグレードする	191
SDXツールファイルをアップロードするには	191
SDXツールをアップグレードするには	192
Websense Protectorインスタンスを新しいバージョンにアップグレードする	192
ソフトウェアイメージをアップロードするには	192
インスタンスをアップグレードするには	192
Websense Protector インスタンスのトラブルシューティング	193
インスタンスに ping を実行するには	193
インスタンスのルートをトレースするには	193
インスタンスを再検出するには	193
BlueCat DNS/DHCP	193
BlueCat DNS/DHCPインスタンスのプロビジョニング	194
BlueCat DNS/DHCPインスタンスを監視する	195
BlueCat DNS/DHCPインスタンスの管理	196

BlueCat DNS/DHCPインスタンスの SDXTools ファイルをアップグレードする	196
BlueCat DNS/DHCPインスタンスを再検出する	197
CAアクセスゲートウェイ	197
CA Access Gateway インスタンスのプロビジョニング	198
CA Access Gateway インスタンスを監視する	199
CA Access Gateway インスタンスを管理する	199
パロアルトネットワークス VMシリーズ	199
Palo Alto VM-Seriesインスタンスのプロビジョニング	200
Palo Alto VM-Seriesインスタンスを監視する	201
Palo Alto VM-Seriesインスタンスを管理する	201
Palo Alto VM-Seriesインスタンスのトラブルシューティング	201
NetScaler SDXアプライアンスにCitrix SD-WAN VPXインスタンスを展開する	203
前提条件	203
Citrix SD-WAN VPXの要件	203
MCNおよびサイトでサポートされるスループット	204
サポートされるスループットのハードウェア要件	204
データセンターのトポロジ	204
NetScaler SDX™ 上でのCitrix SD-WAN VPXインスタンスのプロビジョニング	204
Citrix SD-WAN VPXインスタンスの構成	206
関連情報	206
SDXにおける帯域幅メータリング	207
固定スループットレートの専用帯域幅	207
最小保証スループットと帯域幅バースト機能を備えた専用帯域幅	207
帯域幅割り当てモードの選択	208
VPXインスタンスの最大バースト帯域幅の決定	208
スループットとデータ消費統計の確認	209
NetScalerインスタンスの構成と管理	211
NetScalerインスタンスでSNIPアドレスを作成する	211

NetScalerインスタンスにSNIPアドレスを追加するには	211
構成を保存する	212
NetScalerインスタンスの構成を保存するには	212
NetScalerインスタンスを管理する	212
NetScalerインスタンスを起動、停止、削除、または再起動するには	212
NetScalerインスタンスファイルの削除	213
NetScalerインスタンスファイルを削除するには	213
管理構成を適用する	213
NetScalerインスタンスに管理構成を適用するには	213
SSL証明書のインストールと管理	213
証明書ファイルをSDXアプライアンスにアップロードする	214
SSL証明書ファイルをSDXアプライアンスにアップロードするには	214
SSL証明書ファイルをダウンロードしてバックアップを作成するには	214
SSLキーファイルをSDXアプライアンスにアップロードする	214
SSLキーファイルをSDXアプライアンスにアップロードするには	215
SSLキーファイルをダウンロードしてバックアップを作成するには	215
NetScalerインスタンスへのSSL証明書のインストール	215
NetScalerインスタンスにSSL証明書をインストールするには	215
NetScalerインスタンスでのSSL証明書の更新	216
NetScalerインスタンスでSSL証明書を更新するには	216
NetScalerインスタンスでのSSL証明書のポーリング	217
ポーリング間隔を構成するには	217
即時ポーリングを実行するには	217
NetScalerインスタンスでL2モードを許可する	217
インスタンスでL2モードを許可するには	219
インターフェースでの仮想MACの構成	219
SDX管理サービスでVMACを構成する	220
インターフェースまたはLAチャネルにIPv4またはIPv6 VRIDを追加するには	221

SDXアプライアンスのNetScalerインスタンスで管理パーティションを設定するためのパーティションMACアドレスを生成する	221
VPXインスタンスの変更管理	223
VPXインスタンスの変更管理を表示するには	224
NetScalerインスタンスの構成の更新をポーリングするには	224
NetScalerインスタンスの監査テンプレートを構成するには	224
NetScalerインスタンスの監視	226
VPXインスタンスのプロパティを表示する	226
VPXインスタンスのプロパティを表示するには	226
NetScalerインスタンスの実行中および保存済み構成を表示する	228
NetScalerインスタンスの実行中および保存済み構成を表示するには	228
NetScalerインスタンスをPingする	228
NetScalerインスタンスをPingするには	228
NetScalerインスタンスのルートをトレースする	229
NetScalerインスタンスのルートをトレースするには	229
NetScalerインスタンスを再検出する	229
NetScalerインスタンスを再検出するには	229
ログを使用して操作とイベントを監視する	230
監査ログを表示する	230
タスクログの表示	231
タスクデバイスログの表示	231
タスクコマンドログの表示	232
イベントの表示	232
NetScaler SDXアプライアンスのユースケース	233
Management Service と NetScaler インスタンスが同じネットワークにある場合の統合	233
この例に示すように NetScaler インスタンス 1 をプロビジョニングする	235
管理サービスとNetScalerインスタンスが異なるネットワークにある場合の統合	235
この例に示すように、NetScaler インスタンス 1 をプロビジョニングするには	237

セキュリティゾーン間の統合	237
各インスタンスに専用インターフェースを使用した統合	238
この例に示すように、NetScaler インスタンス 5 と 3 をプロビジョニングするには	240
複数のインスタンスによる物理ポートの共有を伴う統合	240
この例でNetScalerインスタンス7と4をプロビジョニングするには	242
NITRO API	243
NITROパッケージの入手	243
.NET SDK	244
システムAPI	244
構成API	245
リソースの作成	246
リソースの詳細を取得する	247
リソース統計を取得する	248
リソースを更新する	248
リソースを削除する	249
一括操作	250
例外処理	251
REST Webサービス	252
システムAPI	252
構成API	255
リソースの作成	256
リソースの詳細と統計を取得する	257
リソースを更新する	258
リソースを削除する	259
一括操作	259
例外処理	263
NITROの仕組み	263
ジャバ SDK	264

システムAPI	264
構成API	265
リソースの作成	265
リソースの詳細の取得	267
リソース統計の取得	267
リソースの更新	268
リソースの削除	269
一括操作	269
例外処理	271
fix	272

はじめに

NetScaler SDXアプライアンスは、複数のNetScaler仮想マシン（インスタンス）をプロビジョニングおよび管理できるマルチテナントプラットフォームです。SDXアプライアンスは、単一の管理者がアプライアンスを構成および管理し、ホストされている各インスタンスの管理をテナントに委任できるようにすることで、クラウドコンピューティングとマルチテナンシーの要件に対応します。SDXアプライアンスにより、アプライアンス管理者は各テナントに以下の利点を提供できます。

- 1つの完全なインスタンス。各インスタンスには次の特権があります。
 - 専用のCPUおよびメモリリソース
 - エンティティ用の個別のスペース
 - 選択したリリースとビルドを実行する独立性
 - ライフサイクルの独立性
- 完全に分離されたネットワーク。特定のインスタンスを対象とするトラフィックは、そのインスタンスにのみ送信されます。

SDXアプライアンスは、アプライアンスに事前にプロビジョニングされた管理サービスを提供します。管理サービスは、アプライアンス、管理サービス、およびインスタンスを構成、管理、監視するためのユーザーインターフェイス（HTTPおよびHTTPSモード）とAPIを提供します。Citrix®の自己署名証明書は、HTTPSサポートのために事前にパッケージ化されています。Citrixは、管理サービスのユーザーインターフェイスにアクセスするためにHTTPSモードを使用することを推奨します。

リリースノート

リリースノートには、特定のリリースまたはNetScalerソフトウェアのビルドに関する機能強化、変更点、バグ修正、および既知の問題が記載されています。NetScaler SDXのリリースノートは、ADCのリリースノートの一部として扱われます。

SDX 13.1の機能強化、既知の問題、およびバグ修正の詳細については、[ADCリリースノート](#)を参照してください。

Management Serviceユーザーインターフェイスの利用を開始する

アプライアンス、Management Service、および仮想インスタンスの構成、管理、監視を開始するには、ブラウザを使用してManagement Serviceユーザーインターフェイスに接続します。次に、アプライアンスで仮想インスタンスをプロビジョニングします。

Management Serviceユーザーインターフェイスには、次のいずれかのサポートされているブラウザを使用して接続できます。

- インターネット エクスプローラー
- グーグル クローム
- アップル サファリ
- モジラ ファイアフォックス

Management Serviceユーザーインターフェイスにログオンする

1. Webブラウザのアドレスフィールドに、次のいずれかを入力します。

`http://Management Service IP Address`

または

`https://Management Service IP Address`

2. ログインページで、**ユーザー名とパスワード**にManagement Serviceのユーザー名とパスワードを入力します。デフォルトのユーザー名は `nsroot` です。デフォルトのパスワードが機能しない場合は、アプライアンスのシリアル番号を入力してみてください。シリアル番号のバーコードは、アプライアンスの背面にあります。初めてデフォルトの資格情報でログインした後、デフォルトの `nsroot` パスワードを変更する必要があります。管理者パスワードの変更については、「[デフォルトユーザーアカウントのパスワードの変更](#)」を参照してください。
3. をクリックし、次の操作を行います。

- a. **開始ページ**リストで、ユーザーインターフェイスにログオンした直後に表示するページを選択します。使用可能なオプションは、、、、です。たとえば、ログオン時に Management Serviceにページを表示する場合は、**開始ページ**リストで**構成**を選択します。
- b. **Timeout** に、セッションを期限切れにするまでの時間（分、時間、または日単位）を入力します。最小タイムアウト値は15分です。

Start in と **Timeout** の設定はセッション間で保持されます。これらのデフォルト値は、キャッシュをクリアした後にのみ復元されます。

4. **Login** をクリックして、Management Serviceユーザーインターフェイスにログオンします。

初期セットアップウィザード

セットアップウィザードを使用すると、すべての初回設定を単一のフローで完了できます。

ウィザードを使用して、ネットワーク構成の詳細とシステム設定を構成したり、デフォルトの管理者パスワードを変更したり、ライセンスを管理および更新したりできます。

このウィザードを使用して、初期構成時にSDXアプライアンスに指定したネットワーク構成の詳細を変更することもできます。

ウィザードにアクセスするには、**Configuration > System** に移動し、**Set Up Appliance** の下にある **Setup Wizard** をクリックします。以下のパラメーターの値を入力します。

- **インターフェース:** アプライアンスを管理ワークステーションまたはネットワークに接続する管理インターフェース。可能な値: 0/1, 0/2。デフォルト: 0/1。
- **Gateway:** アプライアンスのサブネットからトラフィックを転送するルーターのIPアドレス。
- Management ServiceにIPv4アドレスを使用する場合は、IPv4チェックボックスを選択し、以下のパラメーターの詳細を入力します。
 - **Appliance Management IP:** Webブラウザを使用してManagement Serviceにアクセスするために使用されるIPv4アドレス。
 - **Netmask:** SDXアプライアンスが配置されているサブネットマスク。
- **DNS:** プライマリDNSサーバーのIPv4アドレス。プライマリDNSサーバーではIPv6アドレスはサポートされていません。
- Management ServiceにIPv6アドレスを使用する場合は、IPv6チェックボックスを選択し、以下のパラメーターの詳細を入力します。
 - **マネジメントサービスIPアドレス:** Webブラウザを使用してマネジメントサービスにアクセスするために使用されるIPv6アドレスです。

- 。 **ゲートウェイIPv6アドレス:** アプライアンスのサブネットからトラフィックを転送するルータのIPv4アドレスです。
- **追加DNS**を選択して、プライマリDNSサーバーとは別に、追加のDNSサーバーとしてDNSサーバーのIPアドレスを追加します。IPアドレスはIPv4またはIPv6のいずれかです。



重要！

セキュリティを向上させるため、Citrix®はアプライアンスのサポート機能を無効にしておくことを推奨します。アプライアンスのサポート機能を無効にするには、**システム > ネットワーク構成**に移動し、**アプライアンスのサポート機能を構成**チェックボックスをオフにします。

システム設定で、マネジメントサービスとNetScalerインスタンスがセキュアチャネル経由でのみ通信するように指定できます。マネジメントサービスのユーザーインターフェイスへのアクセスを制限することもできます。クライアントはhttpsを使用してのみマネジメントサービスのユーザーインターフェイスにログオンできます。

マネジメントサービスとCitrix Hypervisorのタイムゾーンを変更できます。デフォルトのタイムゾーンはUTCです。**パスワードの変更**チェックボックスを選択し、新しいパスワードを入力することで、管理者パスワードを変更できます。

ライセンスの管理では、ライセンスを管理および割り当てることができます。ハードウェアシリアル番号（HSN）またはライセンスアクセスコードを使用してライセンスを割り当てることができます。または、ライセンスがすでにローカルコンピューターに存在する場合は、アプライアンスにアップロードできます。

アプライアンス上のライセンスを選択し、**完了**をクリックして初期設定を完了します。

SDXアプライアンス上でのインスタンスのプロビジョニング

マネジメントサービスを使用して、SDXアプライアンスに1つ以上のNetScalerまたはサードパーティインスタンスをプロビジョニングできます。インストールできるインスタンスの数は、購入したライセンスによって異なります。追加されたインスタンスの数がライセンスで指定された数と等しい場合、マネジメントサービスはそれ以上のインスタンスのプロビジョニングを許可しません。

サードパーティインスタンスのプロビジョニングについては、[サードパーティ仮想マシン](#)を参照してください。

コンソールアクセス

マネジメントサービスインターフェイスから、NetScalerインスタンス、マネジメントサービス、Citrix Hypervisor、およびサードパーティVMのコンソールにアクセスできます。このアクセスは、SDXアプライアンスでホストされているインスタンスのデバッグとトラブルシューティングに役立ちます。

VMのコンソールにアクセスするには、インスタンスリストに移動し、リストからVMを選択し、**Action**リストで**Console Access**をクリックします。

Management ServiceまたはCitrix Hypervisorのコンソールにアクセスするには、**Configuration > System**に移動し、**Console Access**の下にある**Management Service**または**Citrix Hypervisor**リンクをクリックします。

注: Internet Explorerブラウザはコンソールアクセスをサポートしていません。Citrixでは、Management Service HTTPSセッションを介してのみコンソールアクセス機能を使用することをお勧めします。

Management Serviceの統計

ダッシュボードには、SDXアプライアンス上のManagement Serviceによるメモリ、CPU、ディスクリソースの使用状況を監視するためのManagement Serviceの統計が含まれるようになりました。



Management ServiceおよびNetScalerインスタンスへのシングルサインオン

ユーザー資格情報を使用してManagement Serviceにログオンした後、インスタンスにログオンするためにユーザー資格情報を再度入力する必要はありません。デフォルトでは、**Timeout**値は30分に設定されており、設定タブは新しいブラウザウィンドウで開かれます。

ホームページの管理

Management Serviceのホームページには、SDXアプライアンスのパフォーマンスとアプライアンスにプロビジョニングされたインスタンスの概要が表示されます。SDXアプライアンスとインスタンスに関する情報は、要件に応じて追加および削除できるガジェットに表示されます。

デフォルトでホームページで利用できるガジェットは次のとおりです。

- **システムリソース:** アプライアンス上のCPUコアの総数、SSLチップの総数、空きSSLチップの数、合計メモリ、および空きメモリを表示します。
- **システムCPU | メモリ使用率 (%):** アプライアンスのCPUとメモリの使用率をグラフィカルな形式で表示します。
- **システムWAN/LANスループット (Mbps):** SDXアプライアンスの受信および送信トラフィックの合計スループットを、リアルタイムでプロットされ、定期的に更新されるグラフで表示します。
- **NetScalerインスタンス:** NetScalerインスタンスのプロパティを表示します。表示されるプロパティは、名前、VM状態、インスタンス状態、IPアドレス、Rx (Mbps)、Tx (Mbps)、HTTP要求/秒、CPU使用率 (%)、およびメモリ使用率 (%) です。注: 初めてログオンする場合、アプライアンスにインスタンスをプロビジョニングしていないため、ホームページにはNetScalerインスタンスに関連するデータは表示されません。
- **ヘルス監視イベント:** イベントの重大度、メッセージ、発生日時とともに、最新の25件のイベントを表示します。

「ホーム」 ページでは、次のことができます。

- NetScalerインスタンスの詳細を表示および非表示にする

「名前」列でインスタンス名をクリックすると、特定のNetScalerインスタンスの詳細を表示したり非表示にしたりできます。「すべて展開」をクリックしてすべてのインスタンスノードを展開したり、「すべて折りたたむ」をクリックしてすべてのインスタンスノードを折りたたんだりすることもできます。

- ガジェットの追加と削除

他のシステム情報を表示するためにガジェットを追加することもできます。

これらのガジェットを追加するには、ホームページの右上隅にある矢印 (<<) ボタンをクリックし、検索ボックスにキーワードを入力して、をクリックします。使用できる文字は、a-z、A-Z、0~9、\、\$、*、_ です。検索ボックスに文字を入力せずに をクリックすると、使用可能なすべてのガジェットが表示されます。ガジェットが表示されたら、 をクリックします。

現在、「ホーム」ページに次のガジェットを追加できます。

- 。 **ハイパーバイザーの詳細:** ハイパーバイザーの詳細ガジェットには、Citrix Hypervisor の稼働時間、エディション、バージョン、iSCSI 修飾名 (IQN)、製品コード、シリアル番号、ビルド日、ビルド番号に関する詳細が表示されます。
- 。 **ライセンス:** ライセンスガジェットには、SDX ハードウェアプラットフォーム、プラットフォームでサポートされるインスタンスの最大数、サポートされる最大スループット (Mbps)、および利用可能なスループット (Mbps) の詳細が表示されます。

デフォルトで「ホーム」ページに表示されているガジェットを削除した場合でも、ガジェットを検索して「ホーム」ページに再度追加できます。

ポート

SDXアプライアンスが正常に機能するためには、次のポートが開いている必要があります。

タイプ	ポート	詳細
TCP	80	受信HTTP (GUIおよびNITRO) リクエストに使用されます。SDX Management Serviceインターフェイスにアクセスするための主要なインターフェイスの1つです。
TCP	443	受信セキュアHTTP (GUIおよびNITRO) リクエストに使用されます。SDX Management Serviceインターフェイスにアクセスするための主要なインターフェイスの1つです。
TCP	22	SDX Management ServiceインターフェイスへのSSHおよびSCPアクセスに使用されます。
UDP	162	SDX Management Serviceインターフェイスは、SDXアプライアンスでホストされているNetScalerインスタンスか

タイプ	ポート	詳細
		らのSNMPトラップをリッスンします。
UDP	161	SDX Management Service インターフェースは SNMP ウォーク/get リクエストをリッスンします。

データガバナンス

NetScaler Console service connectとは何ですか？

NetScaler Application Delivery Management (ADM) Service Connectは、NetScaler SDXアプライアンスをNetScaler Consoleサービスにシームレスにオンボーディングできるようにする機能です。この機能により、NetScaler SDXアプライアンスはNetScaler Consoleサービスに自動的に安全に接続し、システム、使用状況、およびテレメトリデータを送信できます。このデータに基づいて、NetScaler Consoleサービス上のNetScalerインフラストラクチャに関するインサイトと推奨事項が得られます。

NetScaler Consoleサービスコネクト機能を使用し、NetScaler SDXアプライアンスをNetScaler Consoleサービスにオンボーディングすることで、オンプレミスまたはクラウドのいずれにあるNetScalerおよびNetScaler Gatewayのすべてのアセットを管理できます。さらに、パフォーマンスの問題、高いリソース使用率、重大なエラーなどを迅速に特定するのに役立つ豊富な可視化機能を利用できます。NetScaler Consoleサービスは、NetScalerインスタンスとアプリケーションに幅広い機能を提供します。NetScaler Consoleサービスの詳細については、「[NetScaler Application Delivery Management Service](#)」を参照してください。

重要

- このドキュメントはNetScaler SDXアプライアンスに関するものです。NetScalerアプライアンスの詳細については、「[NetScalerアプライアンス用NetScaler Consoleサービスコネクトの概要](#)」を参照してください。
- NetScaler GatewayもNetScaler Consoleサービスコネクト機能をサポートしています。便宜上、NetScaler Gatewayアプライアンスは以降のセクションでは明示的に言及されていません。

注: NetScaler Consoleサービスコネクト機能は、NetScalerインスタンスおよびNetScaler Gatewayインスタンス向けにリリースされています。ただし、NetScaler Consoleサービス上の対応する機能は、今後のリリースで利用可能になります。この機能の価値は、NetScaler Consoleサービスのリリースとともに間もなく発揮されるでしょう。Citrixは、これが実現した際にこの注記を更新します。この新しい機能の利点は、NetScaler Consoleサービスでリリースされ次第利用できるようになります。

NetScaler Console serviceとは何ですか？

NetScaler Consoleサービスは、NetScaler SDXインスタンスに関する分析情報と、アプリケーションの健全性、パフォーマンス、セキュリティに関するキュレーションされた機械学習ベースの推奨事項を提供することで、NetScaler SDXインスタンスの管理、監視、オーケストレーション、自動化、トラブルシューティングを支援するクラウドベースのソリューションです。詳細については、「[NetScaler Consoleサービス概要](#)」を参照してください。

NetScaler Consoleサービスコネクトはどのように有効になりますか？

NetScaler SDXをリリース13.1にインストールまたはアップグレードすると、NetScaler Consoleサービスコネクトはデフォルトで有効になります。

NetScaler Consoleサービスコネクトを使用してどのようなデータが取得されますか？

NetScaler Consoleサービスコネクトを使用して、以下の詳細が取得されます。

- **NetScaler SDXの詳細**
 - 管理IPアドレス
 - プラットフォームの説明
 - プラットフォームの種類
 - ホスト名
 - システムID
 - エンコードされたシリアルID
 - バージョン
 - シリアルID
 - ホストID
 - タイプ
 - ビルドタイプ
- **主要な使用状況メトリック**
 - 管理CPU使用率
 - メモリ使用率

- CPU使用率
- システム稼働時間
- システム日時

データはどのように使用されますか？

データを収集することで、NetScaler は NetScaler SDX インストールに関するタイムリーで詳細なインサイトを提供できます。これには以下が含まれます。

- **主要メトリック。** CPU、メモリ、スループット、SSL スループットに関する主要メトリックの詳細、および NetScaler SDX インスタンス上の異常な動作を強調表示します。
- **重大なエラー。** NetScaler インスタンスで発生した可能性のある重大なエラー。
- **展開に関するアドバイザリ。** スタンドアロンモードで展開されているが、スループットが高く、単一障害点に対して脆弱な NetScaler インスタンスを特定します。

収集されたデータはどのくらいの期間保持されますか？

収集されたデータはすべて、13 か月を超えて保持されることはありません。

NetScaler から NetScaler Console サービス接続機能を無効にしてサービスの使用を終了することを決定した場合、以前に収集されたデータはすべて 30 日後に削除されます。

データの保存場所と安全性？

NetScaler Console サービス接続によって収集されたすべてのデータは、米国、欧州連合、オーストラリアおよびニュージーランド (ANZ) の3つの地域のいずれかに保存されます。詳細については、「[地理的考慮事項](#)」を参照してください。

データは、データベース層で厳格なテナント分離により安全に保存されます。

NetScaler Console サービス接続を無効にする方法？

NetScaler Console サービス接続を介したデータ収集を無効にする場合は、「[NetScaler Console サービス接続を有効/無効にする方法](#)」を参照してください。

NetScaler SDXアプライアンス向け Console Advisory Connectの概要

NetScaler Consoleサービスは、NetScaler SDXアプライアンスの管理、監視、オーケストレーション、自動化、トラブルシューティングを支援するクラウドベースのソリューションです。また、アプリケーションの健全性、パフォーマンス、セキュリティに関する分析情報と、厳選された機械学習ベースの推奨事項も提供します。詳細については、[NetScaler Consoleサービス](#)を参照してください。

Console Advisory Connectは、NetScaler SDXアプライアンスをNetScaler Consoleサービスにシームレスにオンボーディングするための機能です。この機能により、NetScaler SDXアプライアンスとNetScaler Consoleサービスが統合ソリューションとして機能し、お客様に多大なメリットを提供します。

Console Advisory Connect機能により、NetScaler SDXインスタンスはNetScaler Consoleサービスに自動的に接続し、システム、使用状況、テレメトリデータを送信します。このデータを使用して、NetScaler Consoleサービスは、パフォーマンス問題の迅速な特定や高いリソース使用率など、NetScaler SDXインフラストラクチャに関する洞察と推奨事項を提供します。

NetScaler Consoleサービスの機能を活用するために、NetScaler SDXアプライアンスをNetScaler Consoleサービスにオンボーディングすることを選択できます。オンボーディングプロセスではConsole Advisory Connectを使用し、お客様にとってシームレスで迅速なエクスペリエンスを実現します。

注意点

- Console Advisory Connectは、NetScaler MPX、SDX、VPXインスタンス、およびNetScaler Gatewayアプライアンスで利用可能になりました。

詳細については、[データガバナンス](#)を参照してください。

Console Advisory ConnectはNetScaler Consoleサービスをどのようにサポートしますか？

NetScalerのConsole Advisory Connect機能がNetScaler Consoleサービスとどのように連携するかの概要ワークフローを以下に示します。

1. NetScaler SDXアプライアンスのConsole Advisory Connect機能は、定期的なプローブ要求を使用してNetScaler Consoleサービスに自動接続します。
2. この要求にはシステム、使用状況、テレメトリデータが含まれており、これを使用してNetScaler Consoleサービスは、パフォーマンス問題の迅速な特定や高いリソース使用率など、NetScalerインフラストラクチャに関する洞察と推奨事項を提供します。
3. 洞察と推奨事項を確認し、NetScaler SDXアプライアンスの管理を開始するために、NetScaler SDXアプライアンスをNetScaler Consoleサービスにオンボーディングするかどうかを決定できます。
4. オンボーディングを決定すると、Console Advisory Connect機能がオンボーディングをシームレスに完了するのに役立ちます。

Console Advisory ConnectはどのバージョンのNetScalerでサポートされていますか？

Console Advisory Connectは、すべてのNetScalerプラットフォームとすべてのアプライアンスモデル（MPX、VPX、SDX）でサポートされています。NetScalerリリース13.0ビルド64.xx以降、Console Advisory ConnectはNetScaler SDXアプライアンスでデフォルトで有効になっています。

Console Advisory Connectを有効にする方法？

既存のNetScalerのお客様で、NetScalerリリース13.0ビルド64.xxにアップグレードする場合、アップグレードプロセスの一部として、Console Advisory Connectはデフォルトで有効になります。

新規のNetScalerのお客様で、NetScalerリリース13.0ビルド64.xxをインストールする場合、インストールプロセスの一部として、Console Advisory Connectはデフォルトで有効になります。

注

新しいNetScalerアプライアンスとは異なり、既存のNetScaler SDXアプライアンスはCitrix Insight Service (CIS) またはCall Homeを介してルートを見つけます。

Console Advisory Connectを有効化および無効化する方法？

Console Advisory Connectは、CLI、GUI、またはNITRO APIメソッドから有効化および無効化できます。

CLIの使用

CLIを使用してConsole Advisory Connectを有効にするには

コマンドプロンプトで、次のように入力します。

```
set autoreg_setting autoreg=true
```

CLIを使用してConsole Advisory Connectを無効にするには

コマンドプロンプトで、次のように入力します。

```
set autoreg_setting autoreg=false
```

CLIを使用してConsole Advisory Connectの設定を表示するには

```
show autoreg_setting

autoreg: true

is_banner_displayed: true

Done
```

GUIの使用

NetScaler GUI を使用して Console Advisory Connect を無効にするには

1. **System** に移動します。**System** ページで、**System Settings** セクションの下にある **Configure Console Advisory Connect** をクリックします。
2. **Configure NetScaler Console Parameters** ページで、**Enable Console Advisory Connect** のチェックを外し、**OK** をクリックします。



NITRO API の使用

NITRO コマンドを使用して Console Advisory Connect を無効にできます。

```
curl -X PUT -H "Content-Type:application/json" http://192.0.2.10/nitro/v1/config/sdx_autoreg -d '{"sdx_autoreg":{"autoreg":"false"}}' -u nsroot:Test@1
```

NetScaler Console 組み込みエージェントの動作

NetScaler リリース 13.0 ビルド 61.xx 以降、NetScaler SDX インスタンスには、Console Advisory Connect 機能を持つ組み込みエージェントが搭載されています。NetScaler SDX インスタンスで利用可能な NetScaler Console 組み込みエージェントは、アクティブなデーモンのように起動し、NetScaler Console サービスと通信します。NetScaler Console サービスとの通信が確立されると、組み込みエージェントは定期的に最新のソフトウェアバージョンに自動アップグレードされます。

参照

Console Advisory Connect の詳細については、次のトピックを参照してください。

- データガバナンス: [データガバナンス](#)。
- NetScaler Console サービス: [NetScaler Console サービス](#)。

シングルバンドルアップグレード

注: NetScaler SDXアプライアンスをリリース13.1にインストールまたはアップグレードすると、NetScaler Consoleサービス接続はデフォルトで有効になります。詳細については、「データガバナンスとNetScaler Consoleサービス接続」を参照してください。

シングルバンドルアップグレードは、NetScaler VPXインスタンスイメージを除くすべてのコンポーネントを単一のイメージファイルに結合します。このファイルはシングルバンドルイメージ (SBI) と呼ばれます。

注:

Lights Out Management (LOM) ファームウェアはSBIに追加されるため、Citrix®のお客様はLOMを個別にアップグレードする必要はありません。LOMの更新には、アップグレードプロセスに最大30分かかる場合があります。LOMの詳細については、「[NetScaler SDXアプライアンスのLights Out Managementポート](#)」を参照してください。

SDX 9100および16000プラットフォームの場合、新しいLOMファームウェアを含むSBIにアップグレードした後、LOMの更新を手動でトリガーする必要があります。

このイメージを使用すると、すべてのコンポーネントを1つのステップでアップグレードでき、さまざまなコンポーネント間の非互換性の可能性を排除できます。シングルバンドルアップグレードは、アプライアンスが常にCitrix®がテストおよびサポートするバージョンで実行されていることも保証します。すべてのSDXコンポーネントが単一のファイルに結合されているため、SDXイメージファイルはManagement Serviceイメージファイルよりも大きくなります。

イメージのファイル名は `build-sdx-13.1-<build_number>.tgz` の形式です。Management ServiceがSDX 13.1にアップグレードされると、新しいGUIにはCitrix Hypervisorイメージファイル、補足パック、またはホットフィックスをアップロードするオプションが表示されません。これらのオプションがないのは、SDX 13.1が個々のコンポーネントのアップグレードをサポートしていないためです。

注意事項

- シングルバンドルアップグレードは、最大90分かかる多段階プロセスです。

- まず、Management Serviceが提供された新しいバージョンにアップグレードされます。アップグレード中に、Management Serviceへの接続が失われる場合があります。アップグレードのステータスを監視するには、Management Serviceに再接続してください。
- 次に、新しいManagement ServiceがCitrix Hypervisorをアップグレードし、アプライアンスアップグレードの残りの部分を完了します。リリース11.0以降のManagement Serviceは、Citrix Hypervisorの完全なアップグレードを実行できます。
- Citrix Hypervisor™のアップグレード中はアプライアンスを再起動しないでください。
- Citrixは、Citrix Hypervisorのアップグレードを監視するために、Citrix Hypervisorシリアルコンソール (またはLOMコンソール) を使用することを推奨します。

アプライアンス全体を13.1にアップグレードする

注: アップグレードプロセスでは、すべてのVPXインスタンスを含むSDXアプライアンス全体が複数回再起動されます。この手順を実行する前に、VPXインスタンスがHAセットアップにある場合は、すべてのプライマリHAノードをセカンダリノードにフェイルオーバーしてください。HA展開がない場合は、それに応じてダウンタイムを計画してください。

アプライアンスをアップグレードするには:

1. シングルバンドルイメージファイルをアップロードし、**Configuration > Management Service > Software Images** に移動し、**Upload** をクリックします。
2. **設定 > システム > システム管理** に移動します。
3. System Administration グループで、**Upgrade Appliance** をクリックします。アップグレードプロセスには数分かかります。

アップグレード前に、Management Service には次の情報が表示されます。

- シングルバンドルイメージファイル名。
- アプライアンスで実行されているSDXの現在のバージョン。
- アプライアンスをアップグレードする選択されたバージョン。
- アプライアンスのアップグレードにかかるおおよその時間。
- その他の情報。

Upgrade Appliance をクリックする前に、画面に表示されているすべての情報を確認したことを確認してください。アップグレードプロセスが開始されると、中止することはできません。

サポートされているアップグレードパス

工場出荷時のイメージ	12.1へのアップグレード	13.1 にアップグレード	14.1 にアップグレード
10.5 (EoL)	サポートされていません。FRUブートドライブを新しいイメージに交換してください	サポートされていません。FRUブートドライブを新しいイメージに交換してください	サポートされていません。FRUブートドライブを新しいイメージに交換してください
11.0 (EoL)	サポートされていません。FRUブートドライブを新しいイメージに交換してください	サポートされていません。FRUブートドライブを新しいイメージに交換してください	サポートされていません。FRUブートドライブを新しいイメージに交換してください
11.1 (EoL)	サポートされています (12.1-56.x 以降まで)	バージョン 12.1 までのみサポートされています	バージョン 13.1 までのみサポートされています
12.1	推奨されません	サポートされています	バージョン13.1までのみサポート
13.0 (EoL)	サポートされていません。13.0からのアップグレードは避けてください	サポートされていません。13.0からのアップグレードは避けてください	サポートされていません。13.0からのアップグレードは避けてください
13.1	N/A	サポートされています	サポートされています
14.1	N/A	N/A	サポートされています

関連情報

NetScaler SDX ハードウェア-ソフトウェア互換性マトリックス([/ja-jp/citrix-hardware-platforms/sdx/supported-versions.html](https://ja-jp.citrix-hardware-platforms/sdx/supported-versions.html))

NetScalerインスタンスのアップグレード

注記

- NetScaler SDXアプライアンスをリリース13.1にインストールまたはアップグレードすると、NetScaler Consoleサービス接続がデフォルトで有効になります。詳細については、[データガバナンス](#)および[NetScaler Consoleサービス接続](#)を参照してください。
- NetScaler SDXアプライアンスのアップグレードプロセスでは、バージョン13.1ビルド37.x以降、2回の再起動ではなく1回の再起動が必要です。

NetScalerインスタンスをアップグレードするプロセスには、ビルドファイルのアップロードと、その後のNetScalerインスタンスのアップグレードが含まれます。

重要

Management Serviceを使用したADCインスタンスのダウングレードはサポートされていません。ダウングレードするには、インスタンスCLIを使用してください。

NetScalerインスタンスをアップグレードする前に、NetScalerソフトウェアイメージをNetScaler SDXアプライアンスにアップロードします。新しいインスタンスをインストールするには、NetScaler XVAファイルが必要です。

ソフトウェアイメージペインで、次の詳細を表示できます。

- **名前:** NetScalerインスタンスソフトウェアイメージファイルの名前。ファイル名にはリリース番号とビルド番号が含まれます。たとえば、ファイル名build-10-53.5_nc.tgzはリリース10ビルド53.5を指します。
- **最終変更日時:** ファイルが最後に変更された日付。
- **サイズ:** ファイルのサイズ（MB単位）。

ソフトウェアイメージをアップロードするには

1. ナビゲーションペインで、NetScalerを展開し、次にソフトウェアイメージをクリックします。
2. ソフトウェアイメージペインで、アップロードをクリックします。
3. 「NetScalerソフトウェアイメージのアップロード」ダイアログボックスで、「参照」をクリックし、アップロードするNetScalerイメージファイルを選択します。

4. 「**アップロード**」をクリックします。イメージファイルが「NetScalerソフトウェアイメージ」ペインに表示されます。

ビルドファイルをダウンロードしてバックアップを作成するには

1. 「ソフトウェアイメージ」ペインで、ダウンロードするファイルを選択し、「**ダウンロード**」をクリックします。
2. メッセージボックスで、「**保存**」リストから「**名前を付けて保存**」を選択します。
3. 「名前を付けて保存」メッセージボックスで、ファイルを保存する場所を参照し、「**保存**」をクリックします。

XVAファイルをアップロードするには

1. ナビゲーションペインで、NetScalerを展開し、「ソフトウェアイメージ」をクリックします。
2. 「ソフトウェアイメージ」ペインで、「**XVAファイル**」タブの「**アップロード**」をクリックします。
3. 「**NetScaler XVAファイルのアップロード**」ダイアログボックスで、「**参照**」をクリックし、アップロードするNetScaler XVAファイルを選択します。
4. 「**アップロード**」をクリックします。XVAファイルが「**XVAファイル**」ペインに表示されます。

XVAファイルをダウンロードしてバックアップを作成するには

1. 「XVAファイル」ペインで、ダウンロードするファイルを選択し、「**ダウンロード**」をクリックします。
2. メッセージボックスで、「**保存**」リストから「**名前を付けて保存**」を選択します。
3. 「名前を付けて保存」メッセージボックスで、ファイルを保存する場所を参照し、「**保存**」をクリックします。

NetScaler VPXインスタンスのアップグレード

アプライアンスで実行されているVPXインスタンスを1つ以上、Management Serviceを使用してアップグレードできます。インスタンスをアップグレードする前に、正しいビルドがSDXアプライアンスにアップロードされていることを確認してください。

インスタンスのアップグレードを開始する前に、ライセンスフレームワークとライセンスの種類を理解していることを確認してください。ソフトウェアエディションのアップグレード（標準エディションからエンタープライズエディションへ、またはエンタープライズエディションからプラ

チナエディションへなど) には、新しいライセンスが必要になる場合があります。また、以下の点にも注意してください。

- 設定の損失を防ぐため、インスタンスをアップグレードする前に、各インスタンスの設定を保存してください。
- 個々のインスタンスは、インスタンスノードからアップグレードすることもできます。これを行うには、インスタンスノードからインスタンスを選択します。詳細ペインでインスタンスを選択し、ドロップダウンメニューでをクリックします。

重要

- VPXインスタンスをアップグレードするためにVPX GUIではなくSDX Management Serviceを使用する場合、アップグレードイメージはバックアップファイルの一部となり、インスタンスをスムーズに復元できます。
- 設定にクラシックポリシーが含まれている場合、インスタンスのアップグレード中に「Found unsupported classic policies」というエラーが表示されることがあります。そのような場合は、クラシックポリシーをアドバンストポリシーに手動で変換する必要があります。詳細については、「[Netscaler Notice of Status Change Announcement for Classic Policy Based Features and Functionalities](#)」を参照してください。

以下はエラーメッセージの例です。



VPXインスタンスをアップグレードするには

1. **Configuration**タブのナビゲーションペインで、**NetScaler**をクリックします。
2. 詳細ペインの**NetScaler Configuration**で、**Upgrade**をクリックします。
3. **Upgrade NetScaler**ダイアログボックスの**Software Image**で、アップグレードしたいバージョンのNetScalerアップグレードビルドファイルを選択します。
4. **Instance IP Address**ドロップダウンリストから、アップグレードしたいインスタンスのIPアドレスを選択します。
5. **OK**をクリックし、次に**Close**をクリックします。

関連情報

「NetScaler SDX ハードウェア-ソフトウェア互換性マトリックス」 ([/ja-jp/citrix-hardware-platforms/sdx/supported-versions.html](#))

SDXアプライアンスの管理と監視

NetScaler SDXアプライアンスが稼働した後、Management Serviceユーザーインターフェイスからアプライアンスを管理および監視するためのさまざまなタスクを実行できます。

SDXアプライアンスのネットワーク構成を変更する

初期設定時にSDXアプライアンスに提供したネットワーク構成の詳細を変更できます。

SDXアプライアンスのネットワーク構成を変更するには、**System**をクリックします。**System**ページの**Setup Appliance**グループで、**Network Configuration**をクリックし、ウィザードに詳細を入力します。

注: **Network Configuration**でCitrix Hypervisor™へのアクセスを有効にすると、「アクセスは6時間後に自動的に無効になります」という警告メッセージが表示されます。

デフォルトユーザーアカウントのパスワードを変更する

デフォルトのユーザーアカウントは、NetScaler SDXアプライアンスのすべての機能への完全なアクセスを提供します。セキュリティを維持するため、デフォルトの管理者アカウントは必要な場合にのみ使用してください。職務上、完全なアクセスが必要な個人だけが、デフォルトの管理者アカウントのパスワードを知っている必要があります。Citrixは、デフォルトの管理者パスワードを頻繁に変更することを推奨しています。パスワードを紛失した場合は、アプライアンスの設定を工場出荷時のデフォルトに戻すことでパスワードをデフォルトにリセットし、その後パスワードを変更できます。

デフォルトユーザーアカウントのパスワードを変更するには、**System > User Administration > Users**をクリックします。ユーザーを選択し、**Edit**をクリックしてパスワードを変更します。

アプライアンスのタイムゾーンを変更する

Management ServiceとCitrix Hypervisorのタイムゾーンを変更できます。デフォルトのタイムゾーンはUTCです。

タイムゾーンを変更するには、**System**をクリックし、**System Settings**グループで**Change Time Zone**をクリックします。

アプライアンスのホスト名を変更する

System > System Settings > Change Hostnameに移動して、Management Serviceのホスト名を変更できます。Citrix Hypervisorのホスト名は、バックアップ/復元操作中にバックアップおよび復元されます。設定のリセット中、Citrix Hypervisorのホスト名はデフォルト値「netscaler-sdx」にリセットされます。

VLANフィルタリング

VLANフィルタリングは、物理ポートを共有するVPXインスタンス間のデータ分離を提供します。例えば、2つの異なるVLANに2つのVPXインスタンスを設定し、VLANフィルタリングを有効にすると、一方のインスタンスはもう一方のインスタンスのトラフィックを表示できません。VLANフィルタリングが無効になっている場合、すべてのインスタンスはタグ付きまたはタグなしのブロードキャストパケットを見ることができますが、パケットはソフトウェアレベルで破棄されます。VLANフィルタリングが有効になっている場合、各タグ付きブロードキャストパケットは、対応するタグ付きVLANに属するインスタンスのみに到達します。いずれのインスタンスも対応するタグ付きVLANに属していない場合、パケットはハードウェアレベル（NIC）で破棄されます。

インターフェースでVLANフィルタリングが有効になっている場合、そのインターフェースで利用できるタグ付きVLANの数は限られています。10Gインターフェースでは63個のタグ付きVLAN、1Gインターフェースでは32個のタグ付きVLAN。VPXインスタンスは、設定されたVLAN IDを持つパケットのみを受信します。そのインターフェースでVLANフィルターの状態をDISABLEDからENABLEDに変更した場合は、そのインターフェースに関連付けられているVPXインスタンスを再起動してください。

SDXアプライアンスでは、VLANフィルタリングはデフォルトで有効になっています。インターフェースでVLANフィルタリングを無効にすると、そのインターフェースで最大4096個のVLANを設定できます。

注: VLANフィルタリングは、Citrix Hypervisorバージョン6.0を実行しているSDXアプライアンスでのみ無効にできます。

インターフェースでVLANフィルタリングを有効にするには、**System > Interfaces** をクリックします。インターフェースを選択し、**VLAN Filter** をクリックして詳細を入力し、VLANフィルタリングを有効にします。

クロック同期を構成する

ネットワークタイムプロトコル（NTP）同期を有効にすると、管理サービスが再起動されます。SDXアプライアンスのローカルクロックをNTPサーバーと同期するように設定できます。その結果、SDXアプライアンスのクロックは、ネットワーク上の他のサーバーと同じ日付と時刻の設定

になります。アプライアンスが再起動、アップグレード、またはダウングレードされても、クロック同期設定は変更されません。ただし、高可用性セットアップでは、この設定はセカンダリ NetScaler インスタンスには伝播されません。

NTPサーバーを追加したり、認証パラメータを変更したりすると、クロックはすぐに同期されます。NTP同期を明示的に有効または無効にすることもできます。

注: ローカルNTPサーバーがない場合は、公式NTPサイトで公開されているオープンアクセスNTPサーバーのリストを見つけることができます。 <http://www.ntp.org>。NetScalerをパブリックNTPサーバーを使用するように構成する前に、「Rules of Engagement」ページ（すべてのパブリックタイムサーバーページに含まれるリンク）を必ずお読みください。

NTPサーバーを構成するには、**System > NTP Servers** をクリックします。

NTP同期を有効にするには

1. ナビゲーションペインで、**System** を展開し、**NTP Servers** をクリックします。
2. 詳細ペインで、**NTP Synchronization** をクリックします。
3. **NTP Synchronization** ダイアログボックスで、**Enable NTP Sync** を選択します。
4. **OK** をクリックし、次に **Close** をクリックします。

認証オプションを変更するには

1. ナビゲーションペインで、**System**を展開し、**NTP Servers**をクリックします。
2. 詳細ペインで、**Authentication Parameters**をクリックします。
3. **Modify Authentication Options**ダイアログボックスで、次のパラメータを設定します。
 - **Authentication**—NTP認証を有効にします。指定可能な値: YES、NO。デフォルト: YES。
 - **Trusted Key IDs**—信頼されたキーID。NTPサーバーを追加する際に、このリストからキー識別子を選択します。最小値: 1。最大値: 65534。
 - **Revoke Interval**—Autokeyスキームで使用される特定の暗号化値の再ランダム化の間隔を、2の累乗で秒単位で指定します。デフォルト値: 17 ($2^{17}=36$ 時間)。
 - **Automax Interval**—Autokeyプロトコルで使用されるセッションキーリストの再生成の間隔を、2の累乗で秒単位で指定します。デフォルト値: 12 ($2^{12}=1.1$ 時間)。
4. **OK**をクリックし、次に**Close**をクリックします。

SDXアプライアンスのプロパティを表示する

CPUコア数やSSLチップ数、利用可能な合計メモリと空きメモリ、さまざまな製品の詳細などのシステムプロパティを**Configuration**タブで表示します。

SDXアプライアンスのプロパティを表示するには、**Configuration**タブをクリックします。

システムリソース、ハイパーバイザー、ライセンス、およびシステムに関する次の情報を表示できます。

システムリソース:

- **Total CPU Cores**: SDXアプライアンス上のCPUコア数。
- **合計SSLチップ**: SDXアプライアンス上のSSLチップの総数です。
- **空きSSLチップ**: インスタンスに割り当てられていないSSLチップの総数です。
- **合計メモリ (GB)**: アプライアンスの合計メモリ (GB単位) です。
- **空きメモリ (GB)**: アプライアンスの空きメモリ (GB単位) です。

ハイパーバイザー情報:

- **稼働時間**: アプライアンスが最後に再起動されてからの経過時間 (日数、時間、分単位) です。
- **エディション**: SDXアプライアンスにインストールされているCitrix Hypervisorのエディションです。
- **バージョン**: SDXアプライアンスにインストールされているCitrix Hypervisorのバージョンです。
- **iSCSI IQN**: iSCSI修飾名です。
- **製品コード**: Citrix Hypervisorの製品コードです。
- **シリアル番号**: Citrix Hypervisorのシリアル番号です。
- **ビルド日付**: Citrix Hypervisorのビルド日付です。
- **ビルド番号**: Citrix Hypervisorのビルド番号です。
- **補足パック**: SDXアプライアンスにインストールされている補足パックのバージョンです。

ライセンス情報:

- **プラットフォーム**: インストールされているライセンスに基づくハードウェアプラットフォームのモデル番号。

- **最大インスタンス数:** インストールされているライセンスに基づいて、SDXアプライアンスで設定できるインスタンスの最大数。
- **利用可能なインスタンス (共有):** まだ利用可能なCPUコアの数に応じて構成できるインスタンスの数。
- **最大スループット (Mbps):** インストールされているライセンスに基づいて、アプライアンスで達成できる最大スループット。
- **利用可能なスループット (Mbps):** インストールされているライセンスに基づく利用可能なスループット。

システム情報:

- **プラットフォーム:** ハードウェアプラットフォームのモデル番号。
- **製品:** NetScaler®製品の種類。
- **ビルド:** SDXアプライアンスで実行されているNetScalerのリリースとビルド。
- **IPアドレス:** Management ServiceのIPアドレス。
- **ホストID:** Citrix HypervisorホストID。
- **システムID:** Citrix HypervisorシステムID。
- **シリアル番号:** Citrix Hypervisorのシリアル番号。
- **システム時刻:** 日 月 日 時:分:秒 タイムゾーン 年 の形式で表示されるシステム時刻。
- **稼働時間:** Management Serviceが最後に再起動されてからの経過時間（日数、時間、分）。
- **BIOSバージョン:** BIOSバージョン。

アプライアンスのスループットをリアルタイムで表示する

受信および送信トラフィックのSDXアプライアンスの合計スループットは、定期的に更新されるグラフにリアルタイムでプロットされます。デフォルトでは、受信トラフィックと送信トラフィックの両方のスループットがグラフに一緒にプロットされます。

SDXアプライアンスのスループットを表示するには、GUIで**ダッシュボード**をクリックし、****システムスループット (Mbps)****を確認します。

CPUとメモリの使用状況をリアルタイムで表示する

アプライアンスのCPUとメモリの使用状況のグラフを表示できます。グラフはリアルタイムでプロットされ、定期的に更新されます。

SDXアプライアンスのCPUとメモリの使用状況を表示するには、GUIで**ダッシュボード**をクリックし、**管理サービス統計**を確認します。

すべてのコアのCPU使用率を表示する

SDXアプライアンス上の各CPUコアの使用状況を表示できます。

CPUコア使用率ペインには、次の詳細が表示されます。

- **コア番号:** アプライアンス上のCPUコア番号。
- **物理CPU:** そのコアの物理CPU番号。
- **ハイパースレッド:** そのCPUコアに関連付けられているハイパースレッド。
- **インスタンス:** そのCPUコアを使用しているインスタンス。
- **平均コア使用率:** 平均コア使用率（パーセンテージで表示）。

SDXアプライアンスのすべてのコアのCPU使用率を表示するには、GUIで**ダッシュボード**をクリックし、****システムCPU使用率 (%)****を確認します。

SDXアプライアンスにSSL証明書をインストールする

SDXアプライアンスには、デフォルトのSSL証明書が付属しています。セキュリティ上の理由から、この証明書を独自のSSL証明書に置き換えることをお勧めします。そのためには、まずSSL証明書をManagement Serviceにアップロードし、次に証明書をインストールする必要があります。SSL証明書をインストールすると、Management Serviceとの現在のすべてのクライアントセッションが終了します。追加の構成タスクについては、Management Serviceにログインしてください。

SSL証明書をインストールするには、**システム**をクリックします。**アプライアンスのセットアップ**グループで、**SSL証明書のインストール**をクリックし、ウィザードに詳細を入力します。

Management ServiceでSSL証明書を表示する

Management Serviceは、安全なクライアント接続のためにSSL証明書を使用します。有効性ステータス、発行者、サブジェクト、有効期限までの日数、有効期間、バージョン、シリアル番号など、この証明書の詳細を表示します。

SSL証明書を表示するには、**システム**をクリックし、**アプライアンスのセットアップ**グループで、**SSL証明書の表示**をクリックします。

NetScalerインスタンスのSSL証明書とキー

NetScalerインスタンスのSSL証明書とキーの個別のビューにより、使いやすさが向上します。新しいManagement ServiceノードであるSSL証明書ファイルを使用して、NetScalerインスタンスにインストールできるSSL証明書と対応する公開鍵および秘密鍵のペアをアップロードおよび管理します。

NetScalerインスタンスのSSL証明書とキーにアクセスするには、**構成 > NetScaler > SSL証明書ファイル**に移動します。



システム設定を変更する

セキュリティ上の理由から、Management ServiceとVPXインスタンスがセキュアチャネルを介してのみ相互に通信するように指定できます。Management Serviceユーザーインターフェイスへのアクセスを制限することもできます。クライアントは、httpsを使用してのみManagement Serviceユーザーインターフェイスにログオンできます。

システム設定を変更するには、**構成 > システム**をクリックし、システム設定グループで**システム設定の変更**をクリックします。

アプライアンスを再起動する

管理サービスは、SDXアプライアンスを再起動するオプションを提供します。再起動中、アプライアンスはすべてのホストされたインスタンスをシャットダウンし、Citrix Hypervisorを再起動します。Citrix Hypervisorが再起動すると、管理サービスとともにすべてのホストされたインスタンスが起動します。

アプライアンスを再起動するには、> をクリックし、グループで をクリックします。

アプライアンスをシャットダウンする

管理サービスからSDXアプライアンスをシャットダウンできます。

アプライアンスをシャットダウンするには、> をクリックし、グループで をクリックします。

SDX 管理ドメイン

SDX 管理ドメイン機能は、複数の管理ドメインを作成するのに役立ちます。管理ドメインを使用して、異なる部門のリソースを分離できます。したがって、管理ドメインはリソースの制御を改善し、リソースを最適な使用のためにさまざまなドメインに分散できます。

SDXアプライアンスには、CPUコア、データスループット、メモリ、ディスクスペース、SSLチップ、およびプロビジョニング可能な特定の数のインスタンスなど、固定リソースが付属しています。作成できるインスタンスの数は、ライセンスによって異なります。

SDXアプライアンスは、最大3レベルの管理ドメインをサポートします。アプライアンスが出荷されると、すべてのリソースは所有者に割り当てられます。

作成する管理ドメインはすべて、所有者ドメインのサブドメインです。それぞれの場合において、サブドメインのリソースは親ドメインのリソースプールから割り当てられます。管理ドメインのユーザーは、そのドメインのリソースにアクセスできます。彼らは、同じ階層レベルの他のドメインのリソースや、自分のドメインに割り当てられていない親ドメインのリソースにはアクセスできません。ただし、親ドメインのユーザーは、そのドメインのサブドメインのリソースにアクセスできます。

サブドメインへのリソース割り当ての例

表1は、デフォルトのルートドメインのリソースを示しています。SDX管理者は、これらのリソースをサブドメインに割り当てることができます。この場合、管理者は最大で、例えば10個のCPUコアと840GBのディスクスペースを割り当てることができます。

表1. 所有者リソース

CPUコア	10
スループット (Mbps)	18500
メモリ (MB)	87300
ディスクスペース (GB)	840
SSLチップ	36
インスタンス	36

表2は、以下の名前のサブドメインに割り当てられたリソースを示します。 *Test*。このサブドメインには、親ドメインの10個のCPUコアのうち5個が割り当てられており、残りの5個のコアは、オーナーの他のサブドメインに割り当てることができます。

表2。テストドメインのリソース

CPUコア	5
スループット (Mbps)	1024
メモリ (MB)	2048
ディスク容量 (GB)	40
SSLチップ	8
インスタンス	4

サブドメインを作成する場合、*Test* ドメイン管理者は表2に記載されているリソースのみを割り当てることができます。ドメインは3レベルしか作成できないため、*Test* ドメインは1レベルのサブドメインしか持つことができません。

次の図は、表1と表2に記載されている値とは異なる値を使用した、サブドメイン間のリソース割り当ての別の例を示しています。

管理ドメインを作成するには、**Configuration > System > Administrative Domain** に移動し、必要なオプションを選択します。画面の指示に従ってください。新しいドメインが作成されたら、Management Service のログインページを使用してこのドメインにログインし、ドメイン名とユーザー名を入力します。たとえば、NewDomain という名前のドメインを NewUser というユーザーで作成した場合、NewDomain\NewUser としてログインします。

ユーザーをドメインに割り当てる

サブドメインが作成されると、管理者グループと読み取り専用グループの2つのユーザーグループが自動的に作成されます。デフォルトでは、各ユーザーは管理者グループの一部です。ユーザーは複数のグループに追加できます。

SDX 22000 プラットフォームでのRAIDディスク割り当ての管理

NetScaler SDX 22040/22060/22080/22100/22120アプライアンスには、最大8台の物理ディスクをサポートできるRAID（Redundant Array of Independent Disks）コントローラーが搭載されています。複数のディスクは、パフォーマンスの向上だけでなく、信頼性の向上も提供します。SDXアプライアンスは多くの仮想マシンをホストするため、ディスク障害が複数の仮想マシンに影響を与えるため、信頼性は特に重要です。管理サービス上のRAIDコントローラーは、ディスクミラーリングを実装するRAID 1構成をサポートしています。つまり、2つのディスクが同じデータを保持します。RAID 1アレイ内のディスクが故障した場合、そのミラーが直ちに必要なすべてのデータを提供します。

RAID 1ディスクミラーリングは、2つの物理ドライブを1つの論理ドライブに結合します。論理ドライブの使用可能な容量は、その物理ドライブの1つの容量に相当します。たとえば、2つの1テラバイトドライブを組み合わせると、合計使用可能容量が1テラバイトの単一の論理ドライブが作成されます。このドライブの組み合わせは、アプライアンスには単一の論理ドライブとして表示されます。

SDXアプライアンスは、論理ドライブ0と論理ドライブ1を含む構成で出荷されます。論理ドライブ0は管理サービスとCitrix Hypervisorに割り当てられ、論理ドライブ1はプロビジョニングするNetScalerインスタンスに割り当てられます。より多くの物理ドライブを使用するには、新しい論理ドライブを作成する必要があります。

ドライブのプロパティと操作を表示する

SDXアプライアンスは、最大8つの物理ドライブスロット、つまりアプライアンスの両側に4つのスロットのペアをサポートします。物理ドライブをスロットに挿入できます。物理ドライブを使用する前に、それを論理ドライブの一部にする必要があります。

管理サービスでは、**Configuration > System > RAID**画面に、論理ドライブ、物理ドライブ、およびストレージリポジトリのタブが含まれています。

論理ドライブ

Configuration > System > RAID > Logical Drivesタブでは、各論理ドライブの名前、状態、サイズ、およびその構成要素である物理ドライブに関する情報を表示できます。次の表は、仮想ドライブの状態について説明しています。

状態	説明
最適	仮想ドライブの動作状態は良好です。構成されているすべてのドライブがオンラインです。
劣化	仮想ドライブの動作状態は最適ではありません。構成されているドライブの1つが故障しているか、オフラインです。
失敗	仮想ドライブが失敗しました。
オフライン	仮想ドライブがRAIDコントローラーで利用できません。

論理ドライブを選択し、**Show Physical Drive** をクリックすると、その論理ドライブに関連付けられている物理ドライブの詳細も表示できます。

新しい論理ドライブを作成するには

1. **Configuration > System > RAID** に移動し、**Logical Drives** タブを選択します。
2. **Add** をクリックします。
3. **Create Logical Disk** ダイアログボックスで、動作可能な物理ドライブを含む2つのスロットを選択し、**Create** をクリックします。

物理ドライブ

SDXアプライアンスは最大8つの物理スロットをサポートします。つまり、アプライアンスの両側に4つのスロットがペアになっています。**Configuration > System > RAID > Physical Drives** タブでは、次の情報を表示できます。

- **Slot:**—物理ドライブに関連付けられている物理スロット。
- **Size:**—物理ドライブのサイズ。
- **Firmware State:**—ファームウェアの状態。可能な値:
 - **Online, spun up:**—物理ドライブが稼働しており、RAIDによって制御されています。
 - **未構成（良好）:**—物理ドライブは良好な状態であり、論理ドライブペアの一部として追加できます。
 - **未構成（不良）:**—物理ドライブは良好な状態ではなく、論理ドライブの一部として追加できません。
- **外部状態:**—ディスクが空であるかどうかを示します。

- **論理ドライブ**：—関連付けられた論理ドライブ。

物理ドライブペインで、物理ドライブに対して次のアクションを実行できます。

- **初期化**：—ディスクを初期化します。物理ドライブが良好な状態でない場合でも初期化でき、論理ドライブペアの一部として追加する必要があります。
- **再構築**：—ドライブの再構築を開始します。ドライブグループ内のドライブが故障した場合、故障する前にドライブに保存されていたデータを再作成することで、ドライブを再構築できます。RAIDコントローラーは、ドライブグループ内の他のドライブに保存されているデータを再作成します。
- **ドライブの特定**：—アプライアンス上のドライブを特定します。これは、ドライブに関連付けられたドライブアクティビティLEDを点滅させることで示されます。
- **ドライブの特定を停止**：—アプライアンス上のドライブの特定を停止します。
- **取り外し準備**：—選択した物理ドライブを非アクティブ化して、取り外しできるようにします。

ストレージリポジトリ

構成 > システム > RAID > ストレージリポジトリタブで、SDXアプライアンス上のストレージリポジトリのステータスを表示できます。また、接続されていないストレージリポジトリドライブに関する情報を表示したり、そのドライブを選択して**削除**をクリックすることで削除したりできます。ストレージリポジトリタブには、各ストレージリポジトリに関する次の情報が表示されます。

- **名前**：—ストレージリポジトリドライブの名前。
- **ドライブが接続されているか**：—ストレージリポジトリが接続されているかどうか。ドライブが接続されていない場合、**削除**をクリックして削除できます。
- **サイズ**：—ストレージリポジトリのサイズ。
- **使用済み**：—使用中のストレージリポジトリ領域の量。

SDX 22000アプライアンスに論理ドライブを追加する

SDX 22000プラットフォームに追加の論理ドライブを追加するには:

1. Management Serviceにログインします。
2. **Configuration > System > RAID**に移動します。
3. SDX 22000アプライアンスの背面で、2つの空のSSDをスロット番号4と5に挿入します。稼働中のシステムにSSDを追加できます。 **注**: SSDがNetScaler®認定済みであることを確認してください。

4. Management Serviceで、**Configuration > System > RAID**と**Physical Drives**タブに移動します。追加したSSDが表示されます。
5. **Logical Drive**タブに移動し、**Add**をクリックします。
6. **Create Logical Disk**ページで:
 - a. **First Slot**ドロップダウンリストで、4を選択します。
 - b. **Second Slot**ドロップダウンリストで、5を選択します。
 - c. **Create**をクリックします。

注: Management Serviceでは、スロット番号はゼロから始まります。したがって、Management Serviceのスロット番号付けは、物理アプライアンスのスロット番号付けとは異なります。

論理ドライブが作成され、**Logical Drive tab**の下に表示されます。更新アイコンをクリックして、論理ドライブの順序を更新します。

SDX 22000アプライアンスに2番目の論理ドライブを追加する

別の論理ドライブを追加するには、スロット番号6と7にSSDを挿入します。 **論理ディスクの作成**ページで、「**最初のスロット**」リストから6を選択し、「**2番目のスロット**」リストから7を選択します。

故障したSSDドライブを空のSSDドライブと交換する

故障したSSDドライブを空のSSDドライブと交換するには：

1. 「**構成 > システム > RAID**」に移動します。
2. 「**物理ドライブ**」タブで、交換する故障したドライブを選択します。
3. 「**取り外し準備**」をクリックしてドライブを取り外します。
4. 更新アイコンをクリックして、物理ドライブのリストを更新します。
5. スロットから故障したドライブを物理的に取り外します。
6. 故障したSSDを取り外したスロットに、新しいCitrix®検証済みSSDを挿入します。
7. 管理サービスで、「**構成 > システム > RAID**」に移動します。新しいSSDは「**物理ドライブ**」セクションに表示されます。ドライブの再構築プロセスが自動的に開始されます。

更新アイコンをクリックして、再構築プロセスのステータスを確認します。再構築プロセスが完了すると、「**オンライン、スピニングアップ**」ステータスが **ファームウェアの状態列**に表示されます。

SDXライセンスの概要

重要:

ファイルベースのライセンスシステム（手動で管理されるエンタイトルメントとも呼ばれる）は、従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきましたが、April 15, 2026 にサポート終了（EOL）となります。License Activation Service (LAS) は、Citrix製品スイート全体での製品アクティベーションのための次世代テクノロジーです。April 15, 2026 以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法はLASになり、NetScaler Flexedライセンス（CPL/UHMC）、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポートされます。
- NetScaler Console オンプレミス: 14.1-51.x

注: Console オンプレミスの LAS サポートは、リリース 14.1-51.x 以降です。ただし、ファイルベースのライセンスは、April 15 2026 をもって、Console オンプレミス リリース 14.1-51.x 以降および 13.1-60.x 以降では非推奨となります。Console オンプレミス リリース 14.1-51.x またはリリース 13.1-60.x 以降にアップグレードした場合、15th April 2026 までファイルベースのライセンスを引き続き使用できます。ただし、Console オンプレミス 13.1 は LAS をサポートしていないため、15th April 2026 までに Console オンプレミス リリース 14.1-51.x 以降にアップグレードし、LAS に切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他のすべての従来のNetScalerライセンス形式はLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。

LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。

ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrixは、これらの要件に準拠しない場合、Citrixが法律上または衡平法上持つその他の救済措置に加えて、責任

を負うことなくCitrixメンテナンスを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。

ライセンスアクティベーションサービス

License Activation Service (LAS) は、従来のファイルベースのライセンスに代わる新しいクラウドベースのライセンスソリューションです。LASは、CitrixおよびNetScaler製品のアクティベーションのための新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。

注:

LAS はライセンスメカニズムであり、ライセンスタイプではありません。

詳細については、「[License Activation Service](#)」を参照してください。

SDXアプライアンスでのライセンス管理

注:

ライセンスの詳細については、NetScaler SDX Management Serviceのユーザーインターフェイスを参照してください。

NetScaler SDX Management Serviceでは、ハードウェアシリアル番号（HSN）またはライセンスアクセスコードを使用してライセンスを割り当てることができます。Management Serviceソフトウェアは、アプライアンスのシリアル番号を内部的に取得し、Citrixはライセンス購入時にライセンスアクセスコードを電子メールで送信します。

または、ライセンスがすでにローカルコンピューターに存在する場合は、それをアプライアンスにアップロードできます。

ライセンスの返却や再割り当てなど、その他のすべての機能については、ライセンスポータルを使用する必要があります。オプションで、ライセンス割り当てにライセンスポータルを使用することもできます。詳細については、「[Manage Licenses on citrix.com](#)」を参照してください。

SDXライセンスオプションの詳細については、以下を参照してください。

- [適切なプラットフォームとエディションのオプションの選択](#)。
- [ライセンスモデル](#)

注: 永続ライセンスまたはプールライセンスのインストールには、SDXアプライアンスの再起動は必要ありません。

前提条件

ハードウェアシリアル番号またはライセンスアクセスコードを使用してライセンスを割り当てるには、次の手順を実行します。

1. アプライアンスを介してパブリックドメインにアクセスできる必要があります。たとえば、アプライアンスはwww.citrix.comにアクセスできる必要があります。ライセンス割り当てソフトウェアは、ライセンスのためにCitrixライセンスポータルに内部的にアクセスします。パブリックドメインにアクセスするには、Management ServiceのIPアドレスを設定し、DNSサーバーをセットアップする必要があります。
2. ライセンスはハードウェアにリンクされているか、有効なライセンスアクセスコードが必要です。

Management Service を使用したライセンスの割り当て

ライセンスがすでにハードウェアにリンクされている場合、ライセンス割り当てプロセスでハードウェアのシリアル番号を使用できます。そうでない場合は、ライセンスアクセスコードを入力する必要があります。

デプロイの要件に応じて、ライセンスを部分的に割り当てることができます。たとえば、ライセンスファイルに10個のライセンスが含まれているが、現在の要件が6個のライセンスのみである場合、今すぐ6個のライセンスを割り当て、後でさらにライセンスを割り当てることができます。ライセンスファイルに存在するライセンスの総数を超える割り当てはできません。

ライセンスを割り当てるには

1. Webブラウザで、SDXアプライアンスのManagement ServiceのIPアドレスを入力します（例: `<http://10.102.126.251>`）。
2. ユーザー名とパスワードに、管理者資格情報を入力します。
3. **Configuration**タブで、**System > Licenses**に移動します。
4. 詳細ペインで、**Add License File**をクリックします。

5. 次に、いずれかのオプションを選択します。
 - ローカルコンピューターからライセンスファイルをアップロードする（このオプションはデフォルトで選択されています）
 - ライセンスアクセスコードを使用する

- ハードウェアのシリアル番号を使用する



- **ローカルコンピューターからライセンスファイルをアップロードする:** このオプションを選択した場合、**参照**をクリックしてローカルマシンからゼロキャパシティライセンスを選択します。その後、**完了**をクリックします。
 - a. ゼロキャパシティライセンスが正常に適用されると、「**ライセンスモード**」セクションが「**ライセンス**」ページに表示されます。
 - b. 「**プールされたライセンス**」または「**自己管理型プールライセンス**」のいずれかを選択できます。
 - c. 「**ライセンスサーバー名またはIPアドレス**」フィールドに、ライセンスサーバーの詳細を入力します。
 - d. 「**ポート番号**」フィールドに、ライセンスサーバーのポートを入力します。デフォルト値: 27000。
 - e. 「**ライセンスの取得**」をクリックします。
 - f. 「**ライセンスの割り当て**」ウィンドウで、必要なインスタンスと帯域幅を指定し、「**割り当て**」をクリックします。
 - g. 「**ライセンスの管理**」ページで、ライセンスサーバー、ライセンスエディション、およびプールから割り当てられたインスタンスと帯域幅の詳細を表示できます。

注:

NetScalerリリース13.1ビルド30.x以降、NetScaler SDXアプライアンスは自己管理型プールライセンスをサポートしています。このライセンスを使用すると、ライセンスサーバーへのライセンスファイルのアップロードを簡素化および自動化できます。NetScaler Consoleを使用して、共通の帯域幅またはvCPUとインスタンスプールで構成されるライセンスフレームワークを作成できます。

- **ライセンスアクセスコードを使用:** このオプションを選択した場合、「**ライセンスアクセスコード**」フィールドに**LAC**を入力するか、プロキシサーバー経由で接続するためのチェックボックスをオンにします。次に、「**ライセンスの取得**」をクリックします。
 - a. ライセンスを割り当てるために使用するライセンスファイルを選択します。
 - b. 「**割り当て**」列に、割り当てるライセンスの数を入力します。次に、「**ダウンロード**」をクリックします。

ライセンスがダウンロードされると、「**ライセンスファイル**」の下に表示されます。ライセンスファイルを選択し、「**ライセンスの適用**」をクリックします。

- **ハードウェアシリアル番号を使用:** このオプションを選択すると、ソフトウェアはアプライアンスのシリアル番号を内部的に取得し、この番号を使用してライセンスを表示します。
 - a. 「**ライセンスの取得**」をクリックするか、「**プロキシサーバー経由で接続**」のチェックボックスをオンにしてから「**ライセンスの取得**」をクリックします。

ライセンスファイルをダウンロードした後、ライセンスファイルを選択し、「**Apply Licenses**」をクリックします。

プールされたライセンスの詳細については、「[NetScaler SDXの永続ライセンスをNetScalerプール容量にアップグレードする](https://ja-jp.citrix-application-delivery-management-software/current-release/license-server/adc-pooled-capacity/upgrade-perpetual-license-sdx-pooled-capacity.html)」(ja-jp/citrix-application-delivery-management-software/current-release/license-server/adc-pooled-capacity/upgrade-perpetual-license-sdx-pooled-capacity.html)を参照してください。

ライセンスアクティベーションサービス

重要:

従来、さまざまなオンプレミスコンポーネントのアクティベーションに使用されてきたファイルベースのライセンスシステム (手動で管理されるエンタイトルメントとも呼ばれます) は、April 15, 2026にサポート終了 (EOL) となります。ライセンスアクティベーションサービス (LAS) は、Citrix製品スイート全体における製品アクティベーションのための次世代テクノロジーです。April 15, 2026以降、NetScalerインスタンスをアクティベートおよびライセンス供与する唯一の方法はLASになります。LASは、NetScaler Flexedライセンス (CPL/UHMC)、従来のNetScaler Pooledライセンス、およびNetScaler Fixed term Bandwidthライセンスをサポートします。サポートを継続するには、NetScalerおよびNetScaler Consoleの展開がLAS互換バージョンである必要があります。

LAS互換のNetScaler®の最小要件バージョンは次のとおりです。

- NetScaler ADC: 14.1-51.x、13.1-60.x、13.1-37.246 (FIPS)、14.1-66.68 (FIPS)
- NetScaler SVM: 14.1-51.x、13.1-60.x
- NetScaler Console Service: 2025年9月上旬からサポート
- NetScaler Console オンプレミス: 14.1-51.x

注: Console オンプレミスのLASサポートは、リリース14.1-51.x以降です。ただし、ファイルベースのライセンスは、April 15 2026をもって、Console オンプレミスリリース14.1-51.x以降

および13.1-60.x以降では非推奨となります。Console オンプレミスリリース14.1-51.xまたはリリース13.1-60.x以降にアップグレードした場合、15th April 2026までファイルベースのライセンスを引き続き使用できます。ただし、Console オンプレミス13.1はLASをサポートしていないため、15th April 2026までにConsole オンプレミスリリース14.1-51.x以降にアップグレードし、LASに切り替える必要があります。

Pooled vCPU、CICO、永続ライセンスなど、その他の従来のNetScalerライセンスはすべてLASではサポートされません。アクティブなメンテナンスのない永続ライセンスを利用しているNetScalerインスタンスは、上記のソフトウェアバージョンにアップグレードするとライセンスが失効します。

LASベースのライセンスは、法律または規制によって禁止されている地域のお客様には提供されない場合があります。

ご質問やご不明な点がございましたら、カスタマーケアにお問い合わせください。Citrix®は、これらの要件に準拠しない場合、Citrixが法律または衡平法上持つその他の救済措置に加えて、責任を負うことなくCitrix Maintenanceを制限または停止することがあります。これらの要件は、法律または規制によって禁止されている場合は適用されません。

LASへの移行を開始する前に、[NetScaler向けLAS](#)を読むことをお勧めします。これにより、一般的な前提条件、サポートされているライセンスタイプとサポートされていないライセンスタイプ、特定のライセンスおよび展開タイプに対する正確なワークフロー、およびその他の重要な情報を確実に理解できます。

LASは、従来のファイルベースのライセンスに代わる新しいクラウドベースのライセンスソリューションです。LASは、CitrixおよびNetScaler製品のアクティベーションのための新しいモジュールを導入し、ライセンス管理へのシームレスで最新のアプローチを保証します。

注:

LASはライセンスメカニズムであり、ライセンスタイプではありません。LASはNetScaler展開向けの固定期間帯域幅ライセンスをサポートしています。永続ライセンスなど、従来のNetScalerライセンスの他のすべての形式はLASではサポートされていません。

LASのNetScalerバージョン互換性

LASを使用するには、NetScalerが以下のいずれかの最小バージョン以降を実行している必要があります。

- **NetScaler ADC:** 14.1ビルド51.80、13.1ビルド60.29、13.1ビルド37.247 (FIPS)
- **Management Service (NetScaler SVM):** 14.1ビルド51.83、13.1ビルド60.30

注:

SDXアプライアンスの場合、Management Service (SVM) をLAS対応ビルドにアップグレードし、LASベースのライセンスに移行してください。VPXビルドバージョンはLASの互換性に影響しません。

前提条件

LASを使用するには、以下の前提条件を完了していることを確認してください。

- 有効なCitrix Cloudアカウントが必要です。既存のクラウドアカウントに関する詳細情報、または新しいクラウドアカウントのオンボーディングについては、[アカウント管理](#)を参照してください。
- LASアクティベーションワークフローに使用されるCitrix Cloudアカウントにリンクされている組織ID (Org ID) は、有効な購入済みエンタイトルメントを所有している必要があります。現在のエンタイトルメントを表示するには、[エンタイトルメント](#)を参照してください。
- NetScalerがLAS互換バージョンで実行されていることを確認してください。

NetScaler GUIを使用してLASに移行する

次のいずれかに該当する場合は、このセクションで説明されている手順に従ってください。

- ファイルベースのライセンスを使用している固定期間帯域幅のお客様で、固定期間帯域幅のLASベースのライセンスに移行する場合。
- ライセンスのないNetScalerがあり、固定期間帯域幅LASベースのライセンスを使用したい場合。
- ファイルベースのライセンスを使用している永続ライセンスのお客様が、固定期間帯域幅LASベースのライセンスに移行する場合。

ステップ1: NetScaler GUIで、**System > Licenses**に移動し、**LAS Offline Activation**オプションを選択します。

LASオフラインアクティベーション(/en-us/sdx/media/las-offline-activation.png)

ステップ2: LASアクティベーションは、特定のNetScaler SDXインスタンスの一意的ID情報を含むアクティベーション要求ファイルを生成することから始まります。

1. LASアクティベーション要求ファイルを生成するには、**Generate NetScaler SDX activation request**セクションで**Generate**をクリックします。

NetScalerオフラインアクティベーション要求ファイルの生成(/en-us/sdx/media/generate-offline-request-file.png)

2. アクティベーション要求ファイルが生成されたら、**Download**をクリックしてローカルシステムに保存します。

注:

アクティベーション要求ファイルは7日後に期限切れになります。ファイルが有効であることを確認するために、この期間内に**ステップ3**で説明されているアクティベーションプロセスを完了してください。

NetScalerオフラインアクティベーション要求ファイルのダウンロード(/en-us/sdx/media/download-activation-request-file.png)

ステップ3: **ステップ2**で生成されたアクティベーション要求ファイルをCitrix Cloud™ (LAS UI)にアップロードして、NetScalerのライセンスアクティベーションファイルまたはblobを生成します。

1. Citrix Cloudにログインし、**Citrix Cloud > Licensing > NetScaler licenses > NetScaler SDX**に移動します。
2. **ステップ2**で生成されたアクティベーション要求ファイルをアップロードします。
3. ファイルが正常にアップロードされたら、NetScalerに必要なライセンスタイプを選択します。

注:

複数の固定期間帯域幅エンタイトルメントをお持ちの場合、ドロップダウンメニューに利用可能なすべてのエンタイトルメントが表示されます。このNetScalerインスタンスに適切なものを選択してください。

4. ライセンスの種類を選択した後、ライセンスアクティベーションファイルまたはBLOBを生成してダウンロードします。

注:

ライセンスアクティベーションファイルまたはBLOBは、生成から1年間有効です。



ステップ4: NetScaler GUIに戻り、**System > Licenses**に移動し、**LAS Offline Activation**オプションを選択します。

1. **NetScaler SDX**アクティベーションファイルのアップロードセクションで、**Upload File**をクリックして、**ステップ3**で生成されたライセンスアクティベーションファイルまたはBLOBをアップロードします。



2. アクティベーションファイルをアップロードした後、**Yes**をクリックしてアクティベーションを確認します。



ステップ5: NetScaler SDXはLASを通じてライセンスされています。



ステップ6: 継続的な運用を確保するために、ライセンスアクティベーションファイルまたはBLOBを監視および管理します。

ライセンスアクティベーションファイルまたはBLOBは1年間有効です。インターフェイスで、最終更新日またはアクティベーション日と、次の更新日またはアクティベーション日の両方を確認できます。

NetScalerの機能を継続的に維持するには、次の更新期限が切れる前に「**Renew Now**」をクリックし、「**手順2**」から「**手順5**」を繰り返します。

LASを更新(/en-us/sdx/media/las-renewal-date.png)

重要:

ライセンスアクティベーションファイルまたはブLOBを期限内に更新して適用しない場合、NetScalerはライセンスなしの状態になります。

手順7: Citrix Cloudにログインし、**Licensing > NetScaler licenses > NetScaler SDX**に移動して、LASアクティベーションブLOBを表示します。

注:

デフォルトでは、LASはシステム識別子 (`lsguid`) を使用して、アクティベーションブLOBのリスト表示のためにNetScaler展開を識別します。

システム識別子 (`lsguid`) の代わりにホスト名が選択されている場合、ホスト名が「**NetScaler GUI**」フィールドに表示されます。

ホスト名(/en-us/sdx/media/sdx_hostname.png)

注:

LASへの移行が完了したら、SVM上のローカルファイルベースライセンスを削除します。ファイルベースライセンスはSVMフォルダー `/mpsconfig/license` にあり、シェルプロンプトを使用してこのフォルダーから削除する必要があります。

ライセンスアクティベーションファイルの動作と有効期限

ライセンスアクティベーションファイルまたはブロブは、生成日から1年間有効です。お客様は、次の更新日を追跡し、期限が切れる前にファイルを更新する責任があります。

重要:

ライセンスアクティベーションファイルを有効期限前に更新しなかった場合、NetScalerはライセンスなしの状態になります。

ライセンス契約の有効期限

ライセンス契約の有効期限が切れるまでの残り日数は、**System > Licenses > LAS offline activation** に移動すると、**License Entitlement Expiry** の下に表示されます。

ライセンスエンタイトルメントの有効期限(/en-us/sdx/media/las-license-entitlement-expiry.png)

NetScaler がスムーズに機能するように、ライセンス契約の有効期限が切れる前に、ライセンス契約を更新し、[NetScaler GUI を使用した LAS への移行](#) セクションに記載されている手順を完了する必要があります。

重要

- ライセンス契約が期限内に更新されない場合、NetScaler はライセンスなしの状態になります。
- ライセンスの有効期限が切れると、NetScaler インスタンスは通常の動作を停止し、設定の損失やトラフィック処理の完全なシャットダウンが発生します。

LAS ライセンスワークフロー中に LAS に送信される情報

このセクションでは、すべての初期リクエストおよび各 LAS アクティベーションプロブ更新リクエスト中に、アクティベーションプロブの要求の一部として LAS に送信されるすべての情報について詳しく説明します。

次の表は、ライセンスワークフロー中に LAS に送信されるパラメータをまとめたものです。

パラメータ	説明	LAS ワークフローにおける必要性
タイプ	オフライン NetScaler の LAS 展開タイプを識別するためにハードコードされています。	LAS側での追跡用
lsguid/lxid	NetScalerの一意のID	LASバインディングパラメータ
NSIPとホスト名	IP_hostname形式の NetScalerの現在のホスト名	LAS側での追跡用
lsビルド	NetScalerのバージョンとビルド	LAS側での追跡用
リクエスト時間	リクエストパッケージ (tgz) が作成されたときのタイムスタンプ	LASバインディングパラメータ
組織ID	顧客の組織ID	LASバインディングパラメータ
CCID	顧客のCC ID	LASバインディングパラメータ
プラットフォーム	NetScalerのフォームファクタとモデル	LASバインディングパラメータ
バーンイン日	NetScalerのバージョンとビルドのソフトウェアリリース日	LAS側での追跡用
最終アクティベーションID	更新時に送信された以前の LASアクティベーションID	LASバインディングパラメータ

パラメータ	説明	LAS ワークフローにおける必要性
UIバージョン	ファイルの整合性検証を保証します	ファイル整合性検証

LASアクティベーション識別子の構成

NetScaler ADCまたはManagement Service (SVM) 14.1-60.57、NetScaler ADCまたはManagement Service 13.1-61.26、およびNetScaler FIPS 13.1-37.259以降、NetScaler (ADCまたはManagement Service) 展開のLASベースのライセンスワークフローでは、IPアドレスとホスト名を使用しなくなりました。代わりに、LASはシステム識別子 (`lsguid`) を使用して、NetScaler (ADCまたはManagement Service) 展開を一意に識別します。

システム識別子 (`lsguid`) の代わりにホスト名を使用するには、NetScaler GUIから「**Use hostname for LAS activation blob workflow**」オプションを手動で選択します。

LASアクティベーションのホスト名をアクティブ化するには

1. **System > Licenses > LAS Activation** に移動します。
2. 「**Use hostname for LAS activation blob workflow**」トグルをオンにします。



LAS に移行した NetScaler SDX (SVM) を監視するためのベストプラクティス

このセクションでは、NetScaler SDX (SVM) で LAS を使用しており、Fixed Capacity Subscription ライセンスタイプをお持ちの場合に、NetScaler SDX を監視するために従うことができるベストプラクティスについて詳しく説明します。

前提条件

- [NetScaler 用 LAS](#) ページを読み、NetScaler SDX (SVM) での LAS に関する FAQ も含めてください。
- [License Activation Service](#) を読み、LAS 移行を完了してください。
- 関連する通知を設定し、NetScaler SDX (SVM) の GUI と CLI を定期的に監視するようにしてください。

注:

通知の継続的な改善に努め、このドキュメントもそれに応じて更新していく予定です。

LAS アクティベーションプロブの有効期限の監視

SVM GUI と CLI を使用して、LAS アクティベーションプロブの有効期限を追跡し、予期せぬライセンス中断を回避できます。

SVM GUI:

SVM GUI > 構成 > システム > ライセンス > LASオフラインアクティベーション > ADCライセンス に移動し、**今後の更新** を監視してください。



SVM CLI:

`show license` コマンドを使用し、`Expiry Days` パラメータの値を参照できます。

サンプル:

```
show license
```

```
Platform: 9120
```

```
Cluster: false
```

```
Maximum Instances: 4
```

```
Available Instances: 4
```

```
Maximum Throughput (Mbps): 20000
```

```
Available Throughput (Mbps): 20000
```

```
isPooledLicense: false
```

```
Expiry Days: 208
```

```
isLASLicense: false
```

```
isLASFixedLicense: true
```

Done



通知

SVM GUIのバナー:

このGUIバナーは、LASアクティベーションプロブの有効期限が30日以内に迫っている場合、NetScaler SDXインスタンスによってデフォルトでトリガーされます。ユーザーがログインするたびにGUIに表示されます。



SNMPベースの通知

SNMPトラップまたはアラームは、有効期限が近づいている場合は `LicenseExpiry`、すでに期限切れの場合は `LicenseExpired` と名付けられています。SNMPトラップ `LicenseExpiry` は、LASアクティベーションプロブの有効期限が30日以内に迫っている場合、NetScaler SDXインスタンスによってデフォルトでトリガーされます。このトラップは、LASアクティベーションプロブの有効期限の30日前から24時間ごとに生成され、プロブが期限切れになるまで継続されます。

SDX/SVMのSNMPトラップ宛先を設定する必要があります。設定が完了すると、これらのSNMPトラップを受信できます。

サンプル:

```
[EventNotification[#1]] Inside: send_ns_snmp_trap_LicenseExpiry
```



生成されたイベントは、**System > Events** に移動して表示できます。表示されるメッセージは、「LASアクティベーションプロブは `d` 日以内に期限切れになります」です。



ライセンスエンタイトルメントの有効期限（契約の有効期限）の監視

SVM GUI:

「**SVM GUI > 設定 > システム > ライセンス > LASオフラインアクティベーション > ADCライセンス**」に移動し、「**ライセンスエンタイトルメントの有効期限**」を監視します。



通知

SVM GUIのバナー:

SVM GUIのこのバナーは、ライセンスエンタイトルメントの有効期限が30日以内に迫っている場合にNetScaler SDXインスタンスによってトリガーされます。これは、ユーザーがログインするたびにGUIに表示されます。



SNMPベースの通知:

NetScaler SDXは、ライセンスエンタイトルメントの有効期限に関するイベントを生成します。

SNMPトラップまたはアラームは、有効期限が迫っている場合は `LicenseExpiry`、すでに期限切れの場合は `LicenseExpired` という名前です。

SNMPトラップ `LicenseExpiry` は、ライセンスエンタイトルメントの有効期限が30日以内に迫っている場合に、NetScaler SDXインスタンスによってデフォルトでトリガーされます。このトラップは、ライセンスエンタイトルメントの有効期限の30日前から期限切れになるまで、24時間ごとに生成されます。

SDX/SVMのSNMPトラップ宛先を設定する必要があります。設定が完了すると、これらのSNMPトラップを受信します。

これらのイベントを表示するには、「SDX GUI > システム > イベント」に移動します。表示されるメッセージは、「ライセンスエンタイトルメントは `x` 日で期限切れになります」（最新ビルド）または「ライセンスは `x` 日で期限切れになります」（一部の古いビルド）です。



SDXリソースビジュアライザー

NetScaler SDXアプライアンスにNetScalerインスタンスがプロビジョニングされると、CPU、スループット、メモリなどのさまざまなリソースがインスタンスに割り当てられる必要があります。現在のSDXでは、利用可能なさまざまなリソースに関する情報は表示されません。

リソースビジュアライザーを使用すると、インスタンスのプロビジョニングに使用できるすべての利用可能なリソースが単一のダッシュボードに表示されます。利用可能なリソースと使用されているリソースはすべてグラフィカル形式で表示されます。リソースビジュアライザーは、割り当て可能なリソースに加えて、電源ステータスや温度などの他のパラメーターも表示します。

リソースビジュアライザーは、インスタンスが使用しているさまざまなリソースも表示します。インスタンスに関連付けられているさまざまなリソースを表示するには、ビジュアライザーでインスタンス名をクリックします。ビジュアライザーの右側には、利用可能なリソースと使用されているリソースがすべてグラフィカル形式で表示されます。

次の図は、リソースビジュアライザーで取得された詳細を示しています。



インターフェースの管理

「インターフェース」ペインでは、VPXインスタンス上の仮想インターフェースとSDXアプライアンスのマッピングを表示し、インターフェースにMACアドレスを割り当てることができます。

注: ダイレクトアタッチケーブル (DAC) が接続されているインターフェースでは、オートネゴシエーションはサポートされていません。

「インターフェース」ペインのインターフェースリストの「**状態**」列では、UPはインターフェースが正常にトラフィックを受信していることを示します。DOWNは、インターフェースがトラフィックを送受信できないネットワークの問題を示します。

重要: 1 GBを超える接続では、フロー制御は推奨されません。

インターフェースを構成するには

1. 「**構成**」タブのナビゲーションペインで、「**システム**」を展開し、「**インターフェース**」をクリックします。
2. 「**インターフェース**」ペインで、構成するインターフェースをクリックし、「**編集**」をクリックします。
3. 「**インターフェースの構成**」ウィンドウで、次のパラメータの値を指定します。
 - **オートネゴシエーション**— オートネゴシエーションを有効にします。設定可能な値: ON、OFF。デフォルト: ON。
 - **速度**— インターフェースのイーサネット速度 (Mb/秒)。設定可能な値: 10、100、1000、10000。
 - **デュプレックス**— インターフェースのデュプレックス動作のタイプ。設定可能な値: Full、Half、NONE。デフォルト: NONE。
 - **フロー制御オートネゴシエーション**— フロー制御パラメータを自動的にネゴシエートします。設定可能な値: ON、OFF。デフォルト: ON

- **Rxフロー制御**— Rxフロー制御を有効にします。設定可能な値: ON、OFF。デフォルト: ON
- **Txフロー制御**— Txフロー制御を有効にします。設定可能な値: ON、OFF。デフォルト: ON

4. 「OK」をクリックし、「閉じる」をクリックします。

インターフェイスのパラメータをデフォルト値にリセットするには

1. 「構成」タブのナビゲーションペインで、「システム」を展開し、「インターフェイス」をクリックします。
2. 「インターフェイス」ペインで、リセットするインターフェイスをクリックし、「リセット」をクリックします。

VPXインスタンス上の仮想インターフェイスと物理インターフェイスのマッピングを表示する

NetScaler VPXインスタンスでは、GUIとCLIに、インスタンス上の仮想インターフェイスとアプライアンス上の物理インターフェイスのマッピングが表示されます。

VPXインスタンスにログオンした後、構成ユーティリティで、「ネットワーク」に移動し、「インターフェイス」をクリックします。インスタンス上の仮想インターフェイス番号と、アプライアンス上の対応する物理インターフェイス番号が、次の図に示すように、「説明」フィールドに表示されます。

CLIで、`show interface` コマンドを入力します。例：

```
> show interface

1) Interface 10/3 (10G VF Interface, PF 10/4) #2

flags=0xe460 <ENABLED, UP, UP, HAMON, 802.1q>

MTU=1500, native vlan=1, MAC=6e:b6:f5:21:5d:db, uptime 43h03m35s

Actual: media FIBER, speed 10000, duplex FULL, fctl NONE, throughput 10000

RX: Pkts(2547925) Bytes(287996153) Errs(0) Drops(527183) Stalls(0)

TX: Pkts(196) Bytes(8532) Errs(0) Drops(0) Stalls(0)

NIC: InDisc(0) OutDisc(0) Fctls(0) Stalls(0) Hangs(0) Muted(0)
```

```
Bandwidth thresholds are not set.
```

```
...
```

インターフェイスへのMACアドレスの割り当て

SDXアプライアンスでADCインスタンスをプロビジョニングしている間、Citrix Hypervisor™は、そのインスタンスに関連付けられた仮想インターフェイスにMACアドレスを内部的に割り当てます。同じMACアドレスが、同じアプライアンスまたは別のアプライアンス上の別のインスタンスに関連付けられた仮想インターフェイスに割り当てられる可能性があります。重複するMACアドレスの割り当てを防ぐために、一意のMACアドレスを強制できます。

インターフェイスにMACアドレスを割り当てる方法は2つあります。

1. ベースMACアドレスと範囲をインターフェイスに割り当てる：管理サービスは、ベースアドレスと範囲を使用して一意のMACアドレスを割り当てます。
2. グローバルベースMACアドレスを割り当てる：グローバルベースMACアドレスはすべてのインターフェイスに適用されます。管理サービスは、すべてのインターフェイスのMACアドレスを生成します。グローバルベースMACアドレスを設定すると、1Gインターフェイスの範囲は8に設定されます。10Gインターフェイスの範囲は64に設定されます。グローバルベースMACアドレスが00:00:00:00:00:00に設定されている場合のサンプルベースMACアドレスについては、次の表を参照してください。

物理インターフェイス	ベースMACアドレス
0/1	00:00:00:00:00:00
0/2	00:00:00:00:00:08
1/1	00:00:00:00:00:10
1/2	00:00:00:00:00:18
1/3	00:00:00:00:00:20
1/4	00:00:00:00:00:28
1/5	00:00:00:00:00:30
1/6	00:00:00:00:00:38

物理インターフェイス	ベースMACアドレス
1/7	00:00:00:00:00:40
1/8	00:00:00:00:00:48
10/1	00:00:00:00:00:50
10/2	00:00:00:00:00:90

表1. グローバルベースMACアドレスから生成されたベースMACアドレスの例

管理ポートのベースMACアドレスは参照用です。管理サービスは、ベースMACアドレスに基づいて、1/xおよび10/xポートのみのMACアドレスを生成します。

注: ベースMACアドレスをチャンネルに割り当てることはできません。

MACアドレスに関するさまざまな操作を実行するには、**System > Interfaces** をクリックします。インターフェイスを選択し、**Edit** をクリックします。**Configure Interface** ウィンドウでMACアドレス操作を実行します。

SDXアプライアンスの物理インターフェイスを無効または有効にする

SDXアプライアンスの物理インターフェイスを使用していない場合は、管理サービスを使用して物理インターフェイスを無効にできます。この操作はセキュリティ目的で役立ちます。

注: デフォルトでは、SDXアプライアンス上のすべての物理インターフェイスは有効になっています。また、インターフェイスがVPXまたはチャンネルで使用されている場合、そのインターフェイスを無効にすることはできません。

物理インターフェイスを無効にするには：

1. **Configuration** タブで、ナビゲーションペインの**System**を展開し、**Interfaces**をクリックします。
2. **Interfaces** ペインで、無効にするインターフェイスを選択します。
3. **Action** ドロップダウンリストで、**Disable** をクリックします。

無効になっている物理インターフェイスを使用したい場合は、Management Serviceを使用してそのインターフェイスを有効にできます。

無効になっている物理インターフェイスを有効にするには：

1. **Configuration**タブで、ナビゲーションペインの**System**を展開し、**Interfaces**をクリックします。
2. **Interfaces**ペインで、有効にする無効なインターフェイスを選択します。
3. **Action**ドロップダウンリストで、**Enable**をクリックします。

SDXアプライアンスでのジャンボフレーム

NetScaler SDXアプライアンスは、最大9216バイトのIPデータを含むジャンボフレームの送受信をサポートしています。ジャンボフレームは、標準のIP MTUサイズである1500バイトよりも効率的に大きなファイルを転送できます。

NetScaler SDXアプライアンスは、以下の展開シナリオでジャンボフレームを使用できます。

- **ジャンボからジャンボ:** アプライアンスはデータをジャンボフレームとして受信し、ジャンボフレームとして送信します。
- **非ジャンボからジャンボ:** アプライアンスはデータを非ジャンボフレームとして受信し、ジャンボフレームとして送信します。
- **ジャンボから非ジャンボ:** アプライアンスはデータをジャンボフレームとして受信し、非ジャンボフレームとして送信します。

SDXアプライアンスにプロビジョニングされたNetScalerインスタンスは、以下のプロトコルに対するロードバランシング構成でジャンボフレームをサポートしています。

- TCP
- TCP上のその他のプロトコル
- SIP

ジャンボフレームの詳細については、ユースケースを参照してください。

ユースケース: ジャンボからジャンボへのセットアップ

NetScalerインスタンスNS1で構成されたSIPロードバランシング仮想サーバーLBVS-1が、サーバーS1とS2間でSIPトラフィックをロードバランシングするために使用される、ジャンボからジャンボへのセットアップの例を考えてみましょう。クライアントCL1とNS1間の接続、およびNS1とサーバー間の接続はジャンボフレームをサポートしています。

NS1のインターフェイス10/1は、クライアントCL1からのトラフィックを受信または送信します。NS1のインターフェイス10/2は、サーバーS1またはS2からのトラフィックを受信または送信します。NS1のインターフェイス10/1と10/2は、それぞれVLAN 10とVLAN 20の一部です。

ジャンボフレームをサポートするために、インターフェイス10/1、10/2、およびVLAN 10、VLAN 20のMTUは9216に設定されています。

このセットアップ例では、CL1、S1、S2を含む他のすべてのネットワークデバイスも、ジャンボフレームをサポートするように構成されています。

ジャンボ-ジャンボ(/en-us/sdx/media/jumbo_to_jumbo.png)

次の表に、この例で使用されている設定を示します。

エンティティ	名前	詳細
クライアントCL1のIPアドレス	CL1	192.0.2.10
サーバーのIPアドレス	S1	198.51.100.19
	S2	198.51.100.20
インターフェースに指定されたMTU (管理サービスインターフェースを使用) および NS1上のVLAN (CLIを使用)。	10/1	9000
	10/2	9000
	VLAN 10	9000
	VLAN 20	9000
NS1上のサーバーを表すサービス	SVC-S1	IPアドレス: 198.51.100.19; プロトコル: SIP; ポート: 5060
NS1上のサーバーを表すサービス	SVC-S2	IPアドレス: 198.51.100.20; プロトコル: SIP; ポート: 5060
VLAN 10上の負荷分散仮想サーバー	LBVS-1	IPアドレス: 203.0.113.15; プ ロトコル: SIP; ポート: 5060;SVC-S1, SVC-S2

CL1からNS1へのリクエストのトラフィックフローは次のとおりです。

1. CL1はLBVS1に対して20000バイトのSIPリクエストを作成します。
2. CL1は、IPフラグメントでリクエストデータをNS1のLBVS1に送信します。各IPフラグメントのサイズは、CL1がこれらのフラグメントをNS1に送信するインターフェースに設定されたMTU (9000) 以下です。
 - 最初のIPフラグメントのサイズ === 9000
 - 2番目のIPフラグメントのサイズ === 9000
 - 最後のIPフラグメントのサイズ === 2068
3. NS1はインターフェース10/1でリクエストIPフラグメントを受信します。これらのフラグメントの各サイズはインターフェース10/1のMTU (9000) 以下であるため、NS1はこれらのフラグメントを受け入れます。
4. NS1はこれらのIPフラグメントを再構成して27000バイトのSIPリクエストを形成します。NS1はこのリクエストを処理します。
5. LBVS-1の負荷分散アルゴリズムはサーバーS1を選択します。
6. NS1は、IPフラグメントでリクエストデータをS1に送信します。各IPフラグメントのサイズは、NS1がこれらのフラグメントをS1に送信するインターフェース10/2のMTU (9000) 以下です。IPパケットはNS1のSNIPアドレスを送信元としています。
 - 最初のIPフラグメントのサイズ === 9000
 - 2番目のIPフラグメントのサイズ === 9000
 - 最後のIPフラグメントのサイズ === 2068

この例における、CL1に対するS1の応答のトラフィックフローは次のとおりです。

1. サーバーS1は、NS1のSNIPアドレスに送信するために、30000バイトのSIP応答を作成します。
2. S1は応答データをIPフラグメントでNS1に送信します。各IPフラグメントのサイズは、S1がこれらのフラグメントをNS1に送信するインターフェイスに設定されたMTU (9000) 以下です。
 - 最初のIPフラグメントのサイズ === 9000
 - 2番目と3番目のIPフラグメントのサイズ === 9000
 - 最後のIPフラグメントのサイズ === 3088
3. NS1はインターフェイス10/2で応答IPフラグメントを受信します。各フラグメントのサイズがインターフェイス10/2のMTU (9000) 以下であるため、NS1はこれらのフラグメントを受け入れます。

4. NS1はこれらのIPフラグメントを再構成して27000バイトのSIP応答を形成します。NS1はこの応答を処理します。
5. NS1は応答データをIPフラグメントでCL1に送信します。各IPフラグメントのサイズは、NS1がこれらのフラグメントをCL1に送信するインターフェイス10/1のMTU (9000) 以下です。IPフラグメントはLBVS-1のIPアドレスを送信元としています。これらのIPパケットはLBVS-1のIPアドレスから送信され、CL1のIPアドレスを宛先としています。

- 最初のIPフラグメントのサイズ === 9000
- 2番目と3番目のIPフラグメントのサイズ === 9000

最後のIPフラグメントのサイズ === 3088

構成タスク:

SDX管理サービスで、**Configuration > System > Interfaces** ページに移動します。必要なインターフェイスを選択し、**Edit** をクリックします。MTU値を設定し、**OK** をクリックします。

例:

インターフェイス 10/1 の MTU 値を 9000 に、インターフェイス 10/2 の MTU 値を 9000 に設定します。

NetScaler インスタンスにログオンし、ADC コマンドラインインターフェイスを使用して、残りの構成手順を完了します。

次の表に、NetScaler インスタンスで必要な構成を作成するためのタスク、コマンド、および例を示します。

タスク	ADC コマンド構文	例
ジャンボフレームをサポートするために、VLAN を作成し、目的の VLAN の MTU を設定します。	<code>add vlan <id> -mtu <positive_integer>; show</code> <code>vlan <id></code>	<code>add vlan 10 -mtu 9000;</code> <code>add vlan 20 -mtu 9000</code>
インターフェイスを VLAN にバインドします。	<code>bind vlan <id> -ifnum <interface_name>; show</code> <code>vlan <id></code>	<code>bind vlan 10 -ifnum 10/1;</code> <code>bind vlan 20 -ifnum 10/2</code>
SNIP アドレスを追加します。	<code>add ns ip <IPAddress> <netmask> -type SNIP;</code> <code>show ns ip</code>	<code>add ns ip 198.51.100.18 255.255.255.0 -type SNIP</code>

タスク	ADC コマンド構文	例
SIPサーバーを表すサービスを作成します。	<pre>add service <serviceName> <ip> SIP_UDP <port> ; show service <name></pre>	サービス SVC-S1 198.51.100.19 SIP_UDP 5060 を追加します。サービス SVC-S2 198.51.100.20 SIP_UDP 5060 をddします。
SIP負荷分散仮想サーバーを作成し、サービスをそれにバインドします。	<pre>add lb vserver <name> SIP_UDP <ip> <port> ; bind lb vserver <vserverName> <serviceName> ; show lb vserver <name></pre>	<pre>add lb vserver LBVS-1 SIP_UDP 203.0.113.15 5060 ; bind lb vserver LBVS-1 SVC-S1 ; bind lb vserver LBVS-1 SVC-S2</pre>
	<pre>bind lb vserver LBVS-1 SVC-S2</pre> <pre>save ns config ; show ns config</pre>	

ユースケース: 非ジャンボからジャンボへのセットアップ

NetScalerインスタンスNS1で構成された負荷分散仮想サーバーLBVS1が、サーバーS1とS2間でトラフィックを負荷分散するために使用される、非ジャンボからジャンボへのセットアップの例を考えてみましょう。クライアントCL1とNS1間の接続は非ジャンボフレームをサポートし、NS1とサーバー間の接続はジャンボフレームをサポートします。

NS1のインターフェイス10/1は、クライアントCL1からのトラフィックを受信または送信します。NS1のインターフェイス10/2は、サーバーS1またはS2からのトラフィックを受信または送信します。

NS1のインターフェイス10/1と10/2は、それぞれVLAN 10とVLAN 20の一部です。CL1とNS1間で非ジャンボフレームのみをサポートするために、インターフェイス10/1とVLAN 10の両方でMTUはデフォルト値の1500に設定されています。

NS1とサーバー間でジャンボフレームをサポートするために、インターフェイス10/2とVLAN 20のMTUは9000に設定されています。

サーバーおよびNS1とサーバー間の他のすべてのネットワークデバイスも、ジャンボフレームをサポートするように構成されています。HTTPトラフィックはTCPに基づいているため、ジャンボフレームをサポートするために、各エンドポイントでMSSがそれに応じて設定されます。

- CL1とNS1の仮想サーバーLBVS1間の接続の場合、NS1のMSSはTCPプロファイルで設定され、そのプロファイルはLBVS1にバインドされます。

- NS1のSNIPアドレスとS1間の接続の場合、NS1上のMSSはTCPプロファイルで設定され、その後、NS1上のS1を表すサービス (SVC-S1) にバインドされます。



次の表に、この例で使用されている設定を示します。

エンティティ	名前	詳細
クライアントCL1のIPアドレス	CL1	192.0.2.10
サーバーのIPアドレス	S1	198.51.100.19
	S2	198.51.100.20
インターフェイス10/1のMTU (管理サービスインターフェイスを使用)。	1500	
インターフェース 10/2 に設定されたMTU (管理サービスインターフェイスを使用して)。	9000	
NS1 の VLAN 10 の MTU (ADC コマンドラインインターフェイスを使用して)。	1500	
NS1 の VLAN 20 に設定された MTU (ADC コマンドラインインターフェイスを使用して)。	9000	
サーバーを表す NS1 上のサービス	SVC-S1	IPアドレス: 198.51.100.19; プロトコル: HTTP; ポート: 80; MSS: 8960
	SVC-S2	IPアドレス: 198.51.100.20; プロトコル: HTTP; ポート: 80; MSS: 8960
VLAN 10 上の負荷分散仮想サーバー	LBVS-1	IPアドレス: 203.0.113.15; プロトコル: HTTP; ポート: 80. バインドされたサービス:

エンティティ	名前	詳細
		SVC-S1, SVC-S2; MSS: 1460

この例におけるCL1からS1へのトラフィックフローは次のとおりです。

1. クライアントCL1は、NS1の仮想サーバーLBVS-1に送信する200バイトのHTTPリクエストを作成します。
2. CL1はNS1のLBVS-1への接続を開きます。CL1とNS1は、接続確立中にそれぞれのTCP MSS値を交換します。
3. NS1のMSSはHTTPリクエストよりも大きいため、CL1はリクエストデータを単一のIPパケットでNS1に送信します。 1.

```
<div id="concept_57AEA1C9D3DA47948B6D834341388D29__d978e142">
```

```
Size of the request packet = [IP Header + TCP Header + TCP Request] =  
[20 + 20 + 200] = 240
```

```
</div>
```

4. NS1はインターフェース10/1でリクエストパケットを受信し、パケット内のHTTPリクエストデータを処理します。
5. LBVS-1の負荷分散アルゴリズムはサーバーS1を選択し、NS1はそのSNIPアドレスの1つとS1の間に接続を開きます。NS1とCL1は、接続確立中にそれぞれのTCP MSS値を交換します。
6. S1のMSSはHTTPリクエストよりも大きいため、NS1はリクエストデータを単一のIPパケットでS1に送信します。
 - a. リクエストパケットのサイズ = [IPヘッダー + TCPヘッダー + = = 240

この例におけるS1からCL1への応答のトラフィックフローは次のとおりです。

1. サーバーS1は、NS1のSNIPアドレスに送信する18000バイトのHTTP応答を作成します。

2. S1は応答データをNS1のMSSの倍数にセグメント化し、これらのセグメントをIPパケットでNS1に送信します。これらのIPパケットはS1のIPアドレスから発信され、NS1のSNIPアドレス宛てです。
 - 最初の2つのパケットのサイズ === 9000
 - 最後のパケットのサイズ === 2120
3. NS1はインターフェース10/2で応答パケットを受信します。
4. これらのIPパケットから、NS1はすべてのTCPセグメントを組み立てて18000バイトのHTTP応答データを形成します。NS1はこの応答を処理します。
5. NS1は応答データをCL1のMSSの倍数にセグメント化し、これらのセグメントをIPパケットとしてインターフェース10/1からCL1に送信します。これらのIPパケットはLBVS-1のIPアドレスから発信され、CL1のIPアドレス宛てです。
 - 最後のパケットを除くすべてのパケットのサイズ === 1500
 - 最後のパケットのサイズ === 520

構成タスク:

SDX管理サービスで、**Configuration > System > Interfaces**ページに移動します。必要なインターフェースを選択し、**Edit**をクリックします。MTU値を設定し、**OK**をクリックします。

例:

次のMTU値を設定します。

- 10/1インターフェースの場合、1500
- 10/2インターフェースの場合、9000

NetScalerインスタンスにログオンし、ADCコマンドラインインターフェースを使用して残りの構成手順を完了します。

次の表に、NetScalerインスタンスで必要な構成を作成するためのタスク、コマンド、および例を示します。

タスク	ADCコマンドライン構文	例
VLANを作成し、ジャンボフレームをサポートするために必要なVLANのMTUを設定します。	<pre>add vlan <id> -mtu <positive_integer> ; show vlan <id></pre>	<pre>add vlan 10 -mtu 1500 ; add vlan 20 -mtu 9000</pre>

タスク	ADCコマンドライン構文	例
インターフェースをVLANにバインドします。	<code>bind vlan <id> -ifnum <interface_name>; show vlan <id></code>	<code>bind vlan 10 -ifnum 10/1; bind vlan 20 -ifnum 10/2</code>
SNIPアドレスを追加します。	<code>add ns ip <IPAddress> <netmask> -type SNIP; show ns ip</code>	<code>add ns ip 198.51.100.18 255.255.255.0 -type SNIP</code>
HTTPサーバーを表すサービスを作成します	<code>add service <serviceName> <ip> HTTP <port>; show service <name></code>	<code>add service SVC-S1 198.51.100.19 http 80; add service SVC-S2 198.51.100.20 http 80</code>
HTTP負荷分散仮想サーバーを作成し、サービスをそれにバインドします	<code>add lb vserver <name> HTTP <ip> <port>; bind lb vserver <vserverName> <serviceName>; show lb vserver <name></code>	<code>add lb vserver LBVS-1 http 203.0.113.15 80; bind lb vserver LBVS-1 SVC-S1</code>
カスタムTCPプロファイルを作成し、ジャンボフレームをサポートするためにMSSを設定します。	<code>add tcpProfile <name> -mss <positive_integer>; show tcpProfile <name></code>	<code>add tcpprofile NS1-SERVERS-JUMBO -mss 8960</code>
カスタムTCPプロファイルを目的のサービスにバインドします。	<code>set service <Name> -tcpProfileName <string>; show service <name></code>	<code>set service SVC-S1 -tcpProfileName NS1-SERVERS-JUMBO; set service SVC-S2 -tcpProfileName NS1-SERVERS-JUMBO</code>
設定を保存します	<code>save ns config; show ns config</code>	

ユースケース: 同じインターフェースセット上でのジャンボフローと非ジャンボフローの共存

NetScalerインスタンスNS1にロードバランシング仮想サーバーLBVS1とLBVS2が設定されている例を考えます。LBVS1はサーバーS1とS2間のHTTPトラフィックをロードバランシングするため

に使用され、グローバルはサーバーS3とS4間のトラフィックをロードバランシングするために使用されます。

CL1はVLAN 10上にあり、S1とS2はVLAN20上にあり、CL2はVLAN 30上にあり、S3とS4はVLAN 40上にあります。VLAN 10とVLAN 20はジャンボフレームをサポートし、VLAN 30とVLAN 40は非ジャンボフレームのみをサポートします。

言い換えれば、CL1とNS1間の接続、およびNS1とサーバーS1またはS2間の接続はジャンボフレームをサポートします。CL2とNS1間の接続、およびNS1とサーバーS3またはS4間の接続は非ジャンボフレームのみをサポートします。

NS1のインターフェース10/1は、クライアントからのトラフィックまたはクライアントへのトラフィックを受信または送信します。NS1のインターフェース10/2は、サーバーからのトラフィックまたはサーバーへのトラフィックを受信または送信します。

インターフェース10/1は、タグ付きインターフェースとしてVLAN 10とVLAN 20の両方にバインドされています。インターフェース10/2は、タグ付きインターフェースとしてVLAN 30とVLAN 40の両方にバインドされています。

ジャンボフレームをサポートするために、インターフェース10/1と10/2のMTUは9216に設定されています。

NS1では、ジャンボフレームをサポートするためにVLAN 10とVLAN 30のMTUは9000に設定されています。非ジャンボフレームのみをサポートするために、VLAN 20とVLAN 40のMTUはデフォルト値の1500に設定されています。

VLANタグ付きパケットのADCインターフェースにおける実効MTUは、インターフェースのMTUとVLANのMTUのうち、いずれか低い方になります。例:

- インターフェース10/1のMTUは9216です。VLAN 10のMTUは9000です。インターフェース10/1では、VLAN 10タグ付きパケットのMTUは9000です。
- インターフェース10/2のMTUは9216です。VLAN 20のMTUは9000です。インターフェース10/2では、VLAN 20タグ付きパケットのMTUは9000です。
- インターフェース10/1のMTUは9216です。VLAN 30のMTUは1500です。インターフェース10/1では、VLAN 30タグ付きパケットのMTUは1500です。
- インターフェース10/2のMTUは9216です。VLAN 40のMTUは1500です。インターフェース10/2では、VLAN 40タグ付きパケットのMTUは9000です。

CL1、S1、S2、およびCL1とS1またはS2の間にあるすべてのネットワークデバイスは、ジャンボフレーム用に構成されています。

HTTPトラフィックはTCPに基づいているため、ジャンボフレームをサポートするために、各エンドポイントでMSSがそれに応じて設定されます。

- CL1とNS1の仮想サーバーLBVS-1間の接続の場合、NS1のMSSはTCPプロファイルで設定され、その後LBVS1にバインドされます。
- NS1のSNIPアドレスとS1間の接続の場合、NS1のMSSはTCPプロファイルで設定され、その後NS1上のS1を表すサービス (SVC-S1) にバインドされます。

ジャンボ-非ジャンボ(/en-us/sdx/media/coexist_jumbo_nonjumbo.png)

次の表は、この例で使用されている設定を一覧表示します。

エンティティ	名前	詳細
クライアントのIPアドレス	CL1	192.0.2.10
	CL2	192.0.2.20
サーバーのIPアドレス	S1	198.51.100.19
	S2	198.51.100.20
	S3	198.51.101.19
	S4	198.51.101.20
NS1上のSNIPアドレス	198.51.100.18; 198.51.101.18	
NS1上のインターフェースと VLANに指定されたMTU	10/1	9216
	10/2	9216
VLAN 10	9000	
VLAN 20	9000	
VLAN 30	9000	
VLAN 40	1500	
デフォルトTCPプロファイル	nstcp_default_profile	MSS: 1460

エンティティ	名前	詳細
カスタムTCPプロファイル	ALL-JUMBO	MSS: 8960
NS1上のサーバーを表すサービス	SVC-S1	IPアドレス: 198.51.100.19; プロトコル: HTTP; ポート: 80; TCPプロファイル: ALL- JUMBO (MSS: 8960)
	SVC-S2	IPアドレス: 198.51.100.20; プロトコル: HTTP; ポート: 80; TCPプロファイル: ALL- JUMBO (MSS: 8960)
	SVC-S3	IPアドレス: 198.51.101.19; プロトコル: HTTP; ポート: 80; TCPプロファイル: nstcp_default_profile (MSS: 1460)
	SVC-S4	IPアドレス: 198.51.101.20; プロトコル: HTTP; ポート: 80; TCPプロファイル: nstcp_default_profile (MSS: 1460)
NS1上の負荷分散仮想サーバー	LBVS-1	IP address = 203.0.113.15; プ ロトコル: HTTP; ポート: 80. バインドされたサービス: SVC-S1, SVC-S2; TCPプロ ファイル: ALL-JUMBO (MSS: 8960)
	LBVS-2	IP address = 203.0.114.15; プ ロトコル: HTTP; ポート: 80. バインドされたサービス: SVC-S3, SVC-S4; TCPプロ ファイル: nstcp_default_profile (MSS: 1460)

CL1からS1へのリクエストのトラフィックフローは次のとおりです。

1. クライアントCL1は、NS1の仮想サーバーLBVS-1に送信するために、20000バイトのHTTPリクエストを作成します。
2. CL1はNS1のLBVS-1への接続を開きます。CL1とNS1は、接続確立中にTCP MSS値を交換します。
3. NS1のMSS値がHTTPリクエストよりも小さいため、CL1はリクエストデータをNS1のMSSの倍数にセグメント化し、これらのセグメントをVLAN 10としてタグ付けされたIPパケットでNS1に送信します。
 - 最初の2つのパケットのサイズ === 9000
 - 最後のパケットのサイズ === 2120
4. NS1はインターフェース10/1でこれらのパケットを受信します。これらのパケットのサイズは、VLAN 10タグ付きパケットに対するインターフェース10/1の実効MTU (9000) 以下であるため、NS1はこれらのパケットを受け入れます。
5. IPパケットから、NS1はすべてのTCPセグメントを組み立てて20000バイトのHTTPリクエストを形成します。NS1はこのリクエストを処理します。
6. LBVS-1のロードバランシングアルゴリズムはサーバーS1を選択し、NS1はそのSNIPアドレスの1つとS1との間に接続を開きます。NS1とCL1は、接続確立中にそれぞれのTCP MSS値を交換します。
7. NS1はリクエストデータをS1のMSSの倍数にセグメント化し、これらのセグメントをVLAN 20としてタグ付けされたIPパケットでS1に送信します。
 - 最初の2つのパケットのサイズ === 9000
 - 最後のパケットのサイズ === 2120

S1からCL1への応答のトラフィックフローは次のとおりです。

1. サーバーS1は、NS1のSNIPアドレスに送信するために30000バイトのHTTP応答を作成します。
2. S1は応答データをNS1のMSSの倍数にセグメント化し、これらのセグメントをVLAN 20としてタグ付けされたIPパケットでNS1に送信します。これらのIPパケットはS1のIPアドレスから発信され、NS1のSNIPアドレス宛てです。
 - 最初の3つのパケットのサイズ === 9000
 - 最後のパケットのサイズ === 3160

3. NS1はインターフェース10/2で応答パケットを受信します。これらのパケットのサイズは、VLAN 20タグ付きパケットに対するインターフェース10/2の有効なMTU値 (9000) 以下であるため、NS1はこれらのパケットを受け入れます。
4. これらのIPパケットから、NS1はすべてのTCPセグメントを組み立てて30000バイトのHTTP応答を形成します。NS1はこの応答を処理します。
5. NS1は応答データをCL1のMSSの倍数にセグメント化し、これらのセグメントをVLAN 10としてタグ付けされたIPパケットで、インターフェース10/1からCL1に送信します。これらのIPパケットはLBVSのIPアドレスから発信され、CL1のIPアドレス宛てです。

- 最初の3つのパケットのサイズ = [IPヘッダー + TCPヘッダー +] = 9000
- 最後のパケットのサイズ = = 3160

構成タスク:

SDX管理サービスで、**Configuration > System > Interfaces**ページに移動します。必要なインターフェースを選択し、**Edit**をクリックします。MTU値を設定し、**OK**をクリックします。

例:

次のMTU値を設定します。

- 10/1インターフェースの場合、9216
- 10/2インターフェースの場合、9216として

NetScalerインスタンスにログオンし、ADCコマンドラインインターフェースを使用して、残りの設定手順を完了します。

次の表に、NetScalerインスタンスで必要な設定を作成するためのタスク、コマンド、および例を示します。

タスク	構文	例
VLANを作成し、ジャンボフレームをサポートするために必要なVLANのMTUを設定します。	<pre>add vlan <id> -mtu <positive_integer>; show vlan <id></pre>	<pre>add vlan 10 -mtu 9000; add vlan 20 -mtu 9000; add vlan 30 -mtu 1500; add vlan 40 -mtu 1500</pre>
インターフェースをVLANにバインドします。	<pre>bind vlan <id> -ifnum <interface_name>; show vlan <id></pre>	<pre>bind vlan 10 -ifnum 10/1 -tagged; bind vlan 20 -ifnum 10/2</pre>

タスク	構文	例
		<pre>-tagged ; bind vlan 30 -ifnum 10/1 -tagged ; bind vlan 40 -ifnum 10/2 -tagged</pre>
SNIPアドレスを追加します。	<pre>add ns ip <IPAddress> <netmask> -type SNIP ; show ns ip</pre>	<pre>add ns ip 198.51.100.18 255.255.255.0 -type SNIP ; a dd ns ip 198.51.101.18 255.255.255.0 -type SNIP</pre>
HTTPサーバーを表すサービスを作成します。	<pre>add service <serviceName> <ip> HTTP <port> ; show service <name></pre>	<pre>add service SVC-S1 198.51.100.19 http 80 ; add service SVC-S2 198.51.100.20 http 80 ; add service SVC-S3 198.51.101.19 http 80 ; add service SVC-S4 198.51.101.20 http 80</pre>
HTTP負荷分散仮想サーバーを作成し、サービスをそれにバインドします。	<pre>add lb vserver <name> HTTP <ip> <port> ; bind lb vserver <vserverName> <serviceName> ; show lb vserver <name></pre>	<pre>add lb vserver LBVS-1 http 203.0.113.15 80 ; bind lb vserver LBVS-1 SVC-S1 ; bind lb vserver LBVS-1 SVC-S2</pre>
	<pre>add lb vserver LBVS-2 http 203.0.114.15 80 ; bind lb vserver LBVS-2 SVC-S3 ; bind lb vserver LBVS-2 SVC-S4</pre>	
カスタムTCPプロファイルを作成し、ジャンボフレームをサポートするためにそのMSSを設定します。	<pre>add tcpProfile <name> -mss <positive_integer> ; show tcpProfile <name></pre>	<pre>add tcpprofile ALL- JUMBO -mss 8960</pre>
カスタムTCPプロファイルを、目的の負荷分散仮想サーバーとサービスにバインドします。	<pre>set service <Name> -tcpProfileName <string> ; s how service <name></pre>	<pre>set lb vserver LBVS-1 - tcpProfileName ALL-JUMBO ; s et service SVC-S1 - tcpProfileName ALL-JUMBO ; s</pre>

タスク	構文	例
		<pre>et service SVC-S2 - tcpProfileName ALL-JUMBO</pre>
設定を保存します。	<pre>save ns config ; show ns config</pre>	

SDXアプライアンスでのSNMPの設定

NetScaler SDXアプライアンスでSNMPエージェントを設定して、トラップと呼ばれる非同期イベントを生成できます。トラップは、SDXアプライアンスで異常な状態が発生するたびに生成されます。その後、トラップはトラップリスナーと呼ばれるリモートデバイスに送信され、SDXアプライアンスの異常状態を通知します。

SNMPトラップ宛先の構成、MIBファイルのダウンロード、および1つ以上のSNMPマネージャーの構成に加えて、NetScaler SDXアプライアンスをSNMPv3クエリ用に構成できます。

次の図は、SNMPが有効化および構成されているSDXアプライアンスを含むネットワークを示しています。この図では、各SNMPネットワーク管理アプリケーションがSNMPを使用してSDXアプライアンス上のSNMPエージェントと通信します。

図1. SNMPをサポートするSDXアプライアンス

ネットワーク図(/en-us/sdx/media/snmp_architecute.png)

SDXアプライアンス上のSNMPエージェントは、SNMPv2にのみ準拠したトラップを生成します。サポートされているトラップは、SDX MIBファイルで確認できます。このファイルは、SDXユーザーインターフェイスのダウンロードページからダウンロードできます。

SNMPトラップ宛先を追加するには

- 構成タブのナビゲーションペインで、**System > SNMP** を展開し、SNMP Trap Destinations をクリックします。
- SNMP Trap Destinations ペインで、Add をクリックします。
- SNMPトラップ宛先の構成ページで、次のパラメータの値を指定します。
 - 宛先サーバー — SNMPトラップメッセージの送信先となるトラップリスナーのIPv4アドレス。

- **ポート** — トラップリスナーがトラップメッセージをリッスンするUDPポート。トラップリスナーの設定と一致している必要があります。一致しない場合、リスナーはメッセージを破棄します。最小値: 1。デフォルト: 162。
- **コミュニティ** — トラップリスナーがメッセージを認証できるように、トラップメッセージとともに送信されるパスワード（文字列）。文字、数字、ハイフン (-)、ピリオド (.)、ハッシュ (#)、スペース ()、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア (_) の文字を含めることができます。注: トラップリスナーデバイスで同じコミュニティ文字列を指定してください。そうしないと、リスナーはメッセージを破棄します。デフォルト: public。

4. Add をクリックし、次に Close をクリックします。追加したSNMPトラップ宛先がSNMP Traps ペインに表示されます。

SNMPトラップ宛先のパラメータの値を変更するには、ペインで、変更するトラップ宛先を選択し、をクリックします。ダイアログボックスで、パラメータを変更します。

SNMPトラップを削除するには、ペインで、削除するトラップ宛先を選択し、をクリックします。メッセージボックスで、クリックしてSNMPトラップ宛先を削除します。

MIBファイルのダウンロード

SDXアプライアンスの監視を開始する前に、次のファイルをダウンロードする必要があります。

SDX-MIB-smiv2.mib。 このファイルは、SNMPv2マネージャーおよびSNMPv2トラップリスナーによって使用されます。

このファイルには、SDX固有のイベントを提供するNetScalerエンタープライズMIBが含まれています。

MIBファイルをダウンロードするには

1. SDXアプライアンスのユーザーインターフェイスのページにログインします。
2. の下で、をクリックします。MIBブラウザを使用してファイルを開くことができます。

SNMPマネージャーコミュニティの追加

SDXアプライアンスでSNMPマネージャーを設定して、アプライアンスおよびアプライアンスでホストされている管理対象デバイスを照会および監視します。また、SNMPマネージャーに必要なアプライアンス固有の情報を提供する必要があります。IPv4 SNMPマネージャーの場合、マネージャーのIPアドレスの代わりにホスト名を指定できます。その場合、SNMPマネージャーのホスト名をそのIPアドレスに解決するDNSネームサーバーを追加する必要があります。

少なくとも1つのSNMPマネージャーを設定します。SNMPマネージャーを設定しない場合、アプライアンスはネットワーク上のどのIPアドレスからのSNMPクエリも受け入れず、応答しません。1つ以上のSNMPマネージャーを設定した場合、アプライアンスはそれらの特定のIPアドレスからのSNMPクエリのみを受け入れ、応答します。

SNMPマネージャーを設定するには

1. タブのナビゲーションペインで、 を展開し、次に を展開します。
2.  をクリックします。
3. 詳細ペインで、 をクリックします。
4. ページで、次のパラメータを設定します。
 - **SNMPマネージャー** — SNMPマネージャーのIPv4アドレス。または、IPv4アドレスの代わりに、SNMPマネージャーに割り当てられているホスト名を指定することもできます。その場合は、SNMPマネージャーのホスト名をIPアドレスに解決するDNSネームサーバーを追加する必要があります。
 - **コミュニティ** — SNMPコミュニティ文字列。大文字と小文字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア (_) の文字を含む1〜31文字で構成できます。
 - **ネットマスク**を使用してSNMPマネージャーを指定するには、☐ チェックボックスをオンにします。
 - フィールドに、SNMPコミュニティのネットマスクを入力します。
5.  をクリックし、 をクリックします。

SNMPv3クエリ用のSDXアプライアンスの構成

SNMPv3は、SNMPv1およびSNMPv2の基本的な構造とアーキテクチャに基づいています。ただし、SNMPv3は、認証、アクセス制御、データ整合性チェック、データ発信元検証、メッセージ適時性チェック、データ機密性などの管理およびセキュリティ機能を組み込むために、基本的なアーキテクチャを強化しています。

NetScaler SDXアプライアンスは、SNMPv3のセキュリティ機能を実装できる次のエンティティをサポートしています。

- SNMPビュー
- SNMPユーザー

これらのエンティティは連携してSNMPv3セキュリティ機能を実装します。ビューは、MIBのサブツリーへのアクセスを許可するために作成されます。

SNMPマネージャーの追加

適切なSNMPマネージャーがSDXアプライアンスをクエリできるように構成します。また、SNMPマネージャーに必要なアプライアンス固有の情報を提供します。IPv4 SNMPマネージャーの場合、マネージャーのIPアドレスの代わりにホスト名を指定できます。その場合は、SNMPマネージャーのホスト名をIPアドレスに解決するDNSネームサーバーを追加する必要があります。

少なくとも1つのSNMPマネージャーを設定します。SNMPマネージャーを設定しない場合、アプライアンスはネットワーク上のどのIPアドレスからのSNMPクエリも受け入れず、応答もしません。1つ以上のSNMPマネージャーを設定した場合、アプライアンスはそれらの特定のIPアドレスからのSNMPクエリのみを受け入れ、応答します。

SNMPマネージャーを設定するには：

1. **System > Configuration** ページに移動します。
2. Configurationタブのナビゲーションペインで、Systemを展開し、次にSNMPを展開します。
3. Managersをクリックします。
4. 詳細ペインで、Addをクリックします。
5. Add SNMP Manager Communityダイアログボックスで、次のパラメーターを設定します。
 - **SNMPマネージャー**—SNMPマネージャーのIPv4アドレス。または、IPv4アドレスの代わりに、SNMPマネージャーに割り当てられているホスト名を指定することもできます。その場合、SNMPマネージャーのホスト名をIPアドレスに解決するDNSネームサーバーを追加する必要があります。
 - **コミュニティ**—SNMPコミュニティ文字列。大文字と小文字の英字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、アットマーク (@)、等号 (=)、コロンの (:)、アンダースコア (_) の文字を含む1~31文字で構成できます。
6. Addをクリックし、次にCloseをクリックします。

SNMPビューの設定

SNMPビューは、MIBの特定のセクションへのユーザーアクセスを制限します。SNMPビューはアクセス制御を実装するために使用されます。

ビューを設定するには

1. Configurationタブのナビゲーションペインで、Systemを展開し、次にSNMPを展開します。

2. Viewsをクリックします。
3. 詳細ペインで、 をクリックします。
4. ダイアログボックスで、次のパラメータを設定します。
 - 名前—SNMPv3ビューの名前。大文字と小文字の英字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア (_) の文字を含む1～31文字で構成できます。SNMPv3ビューを識別しやすい名前を選択してください。
 - サブツリー—このSNMPv3ビューに関連付けるMIBツリーの特定のブランチ（サブツリー）。サブツリーをSNMP OIDとして指定します。
 - タイプ—サブツリーパラメータで指定されたサブツリーを、このビューに含めるか除外するか。この設定は、SNMPv3ビューにAのようなサブツリーを含め、Aの特定のサブツリー（Bなど）をSNMPv3ビューから除外したい場合に役立ちます。

SNMPユーザーの構成

SNMPビューを作成したら、SNMPユーザーを追加します。SNMPユーザーは、SNMPマネージャーのクエリに必要なMIBにアクセスできます。

ユーザーを構成するには

1. タブのナビゲーションペインで、 を展開し、次に を展開します。
2. をクリックします。
3. 詳細ペインで、 をクリックします。
4. ページで、次のパラメータを設定します。
 - 名前—SNMPv3ユーザーの名前。大文字と小文字の英字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、アットマーク (@)、等号 (=)、コロン (:)、アンダースコア (_) の文字を含む1～31文字で構成できます。
 - セキュリティレベル—アプライアンスとSNMPv3ユーザー間の通信に必要なセキュリティレベル。次のいずれかのオプションから選択します。
 - noAuthNoPriv—認証も暗号化も不要です。
 - authNoPriv—認証は必要ですが、暗号化は不要です。
 - authPriv—認証と暗号化が必要です。
 - 認証プロトコル—アプライアンスとSNMPv3ユーザー間の通信を認証するために使用される認証アルゴリズム。SNMPマネージャーでSNMPv3ユーザーを設定する際には、同じ認証アルゴリズムを指定してください。

- 認証パスワード—認証アルゴリズムで使用するパスフレーズ。大文字と小文字の英字、数字、ハイフン (-)、ピリオド (.)、ポンド (#)、スペース ()、アットマーク (@)、等号 (=)、コロンの (:)、アンダースコア () の文字を含む1~31文字で構成できます。
- プライバシープロトコル—アプライアンスとSNMPv3ユーザー間の通信を暗号化するために使用される暗号化アルゴリズム。SNMPマネージャーでSNMPv3ユーザーを設定する際には、同じ暗号化アルゴリズムを指定してください。
- ビュー名—このSNMPv3ユーザーにバインドする、設定済みのSNMPv3ビューの名前。SNMPv3ユーザーは、このSNMPv3ビューにINCLUDEDタイプとしてバインドされているサブツリーにはアクセスできますが、EXCLUDEDタイプのサブツリーにはアクセスできません。

SNMPアラームの設定

アプライアンスは、SNMPアラームと呼ばれる事前定義された条件エンティティのセットを提供します。SNMPアラームの条件セットが満たされると、アプライアンスは設定されたトラップリスナーに送信されるSNMPトラップメッセージを生成します。たとえば、deviceAddedアラームが有効になっている場合、アプライアンスでデバイス（インスタンス）がプロビジョニングされるたびに、トラップメッセージが生成され、トラップリスナーに送信されます。SNMPアラームに重大度レベルを割り当てることができます。そうすると、対応するトラップメッセージにその重大度レベルが割り当てられます。

アプライアンスで定義されている重大度レベルを、重大度の高い順に示します。

- 緊急
- 主要
- 軽微
- 警告
- 情報 (デフォルト)

たとえば、deviceAddedという名前のSNMPアラームに警告の重大度レベルを設定した場合、デバイスが追加されたときに生成されるトラップメッセージには、警告の重大度レベルが割り当てられます。

SNMPアラームを設定して、そのアラームの条件が満たされるたびに生成される対応するトラップメッセージをログに記録することもできます。

定義済みのSNMPアラームを変更するには、**System > SNMP > Alarms** をクリックします。

syslog通知を設定する

SYSLOGは標準的なロギングプロトコルです。これには2つのコンポーネントがあります。

NetScaler SDXアプライアンス上で動作するSYSLOG監査モジュールと、リモートシステム上で動作可能なSYSLOGサーバーです。SYSLOGはデータ転送にUDPを使用します。

SYSLOGサーバーを実行すると、SDXアプライアンスに接続されます。アプライアンスはすべてのログ情報をSYSLOGサーバーに送信し始め、サーバーはログエントリをログファイルに保存する前にフィルタリングできます。1つのSYSLOGサーバーは複数のSDXアプライアンスからログ情報を受信でき、1つのSDXアプライアンスは複数のSYSLOGサーバーにログ情報を送信できます。

SYSLOGサーバーがSDXアプライアンスから収集するログ情報は、メッセージ形式でログファイルに保存されます。これらのメッセージには通常、以下の情報が含まれます。

- ログメッセージを生成したSDXアプライアンスのIPアドレス
- タイムスタンプ
- メッセージタイプ
- ログレベル（致命的、エラー、通知、警告、情報、デバッグ、警報、または緊急）
- メッセージ情報

この情報を使用して、アラートの原因を分析し、必要に応じて是正措置を講じることができます。まず、アプライアンスがログ情報を送信するsyslogサーバーを設定し、次にログメッセージを記録するためのデータと時刻の形式を指定します。

syslogサーバーを設定する

1. **System > Notifications > Syslog Servers** に移動します。
2. 詳細ペインで、**Add** をクリックします。
3. **Create Syslog Server** ページで、syslogサーバーのパラメータの値を指定します。パラメータの説明については、対応するフィールドにマウスを合わせます。
4. **Add** をクリックし、次に **Close** をクリックします。

syslog パラメータを構成する

1. システム > 通知 > Syslog サーバー に移動します。
2. 詳細ペインで、**Syslog パラメータ** をクリックします。
3. **Syslog パラメータの構成** ページで、日付と時刻の形式を指定します。
4. **OK** をクリックし、次に **閉じる** をクリックします。

メール通知の構成

アラートが生成されるたびにメールメッセージを受信するようにSMTPサーバーを構成します。まずSMTPサーバーを構成し、次にメールプロファイルを構成します。メールプロファイルでは、受信者のアドレスをコンマで区切って指定します。

SMTPサーバーを構成するには

1. 「**System > Notifications > Email**」に移動します。
2. 詳細ペインで、「**Email Server**」タブをクリックし、次に「**Add**」をクリックします。
3. 「**Create Email Server**」ページで、サーバーパラメーターの値を指定します。
 - **サーバー名 / IPアドレス**: SMTPメールサーバーのサーバー名またはIPアドレスを入力します。
 - **ポート**: ポート番号を入力します。デフォルト値は25です。
 - **認証**: メールサーバーへのアクセスを認証するには、このオプションを選択します。
 - **セキュア**: セキュアなメール接続を作成するには、このオプションを選択します。デフォルトでは、TLS 1.2がメール通信の暗号化に使用されます。
4. 「**Create**」をクリックします。

メールプロファイルを構成するには

1. 「**System > Notifications > Email**」に移動します。
2. 詳細ペインで、「**Email**」タブをクリックし、次に「**Add**」をクリックします。
3. 「**Create Email Distribution List**」ページで、パラメーターの値を指定します。パラメーターの説明については、対応するフィールドにマウスカーソルを合わせます。
4. **作成**をクリックします。

SMS通知を構成する

アラートが生成されるたびにSMSメッセージを受信するように、ショートメッセージサービス (SMS) サーバーを構成します。まずSMSサーバーを構成し、次にSMSプロファイルを構成します。SMSプロファイルでは、受信者のアドレスをコンマで区切ります。

SMSサーバーを構成する

1. 「**System > Notifications > SMS**」に移動します。
2. 詳細ペインで、「**SMS Server**」をクリックし、その後「**Add**」をクリックします。

3. 「**Create SMS Server**」 ページで、SMSサーバーパラメーターの値を指定します。これらのパラメーターの値は、ベンダーによって提供されます。
4. 「**Create**」 をクリックし、その後「**Close**」 をクリックします。

SMSプロファイルを構成する

1. 「**System > Notifications > SMS**」 に移動します。
2. 詳細ペインで、「**SMS Distribution List**」 をクリックし、その後「**Add**」 をクリックします。
3. 「**Create SMS Distribution List**」 ページで、メールプロファイルパラメーターの値を指定します。パラメーターの説明については、対応するフィールドにマウスを合わせます。
4. 「**Create**」 をクリックし、その後「**Close**」 をクリックします。

SDXアプライアンスで構成されたエンティティのリアルタイムステータスを監視および管理する

NetScaler SDXアプライアンスは、SDXアプライアンスでホストされている仮想アプライアンス全体の仮想サーバー、サービス、サービスグループ、およびサーバーの状態を監視および管理できます。仮想サーバーの健全性や、サービスまたはサービスグループの最後の状態変更からの経過時間などの値を監視できます。この監視により、エンティティのリアルタイムステータスが可視化され、NetScalerインスタンスに多数のエンティティが構成されている場合に、これらのエンティティの管理が容易になります。



仮想サーバーのステータスを表示する

仮想サーバーの状態と健全性のリアルタイム値を監視できます。また、名前、IPアドレス、仮想サーバーのタイプなど、仮想サーバーの属性を表示することもできます。

- 仮想サーバーのステータスを表示するには
 - a. タブのナビゲーションペインで、**>>** をクリックします。
 - b. 右側のペインの で、次の統計情報を表示します。
 - デバイス名—仮想サーバーが構成されているVPXの名前。
 - 名前—仮想サーバーの名前。
 - プロトコル—仮想サーバーのサービスタイプ。たとえば、HTTP、TCP、SSLなど。
 - 有効な状態—バックアップ仮想サーバーの状態に基づいた、仮想サーバーの有効な状態。たとえば、UP、DOWN、またはOUT OF SERVICE。

- 。状態—仮想サーバーの現在の状態。たとえば、UP、DOWN、またはOUT OF SERVICE。
- 。健全性—UP状態であり、仮想サーバーにバインドされているサービスの割合。健全性パーセンテージの計算には、次の式が使用されます。(バインドされたUPサービスの数 * 100) / バインドされたサービスの合計
- 。IPアドレス—仮想サーバーのIPアドレス。クライアントはこのIPアドレスに接続要求を送信します。
- 。ポート — 仮想サーバーがクライアント接続をリッスンするポート。
- 。最終状態変更 — 仮想サーバーの状態が最後に変更されてからの経過時間 (日、時間、分、秒)。つまり、仮想サーバーが現在の状態であった期間です。この情報は、NetScaler リリース 9.0 以降で構成された仮想サーバーでのみ利用可能です。



- 仮想サーバーにバインドされているサービスとサービスグループの表示

仮想サーバーにバインドされているサービスとサービスグループのリアルタイムステータスを監視できます。この監視により、仮想サーバーの健全性パーセンテージが低下する可能性のあるサービスの状態を確認し、適切な措置を講じることができます。

仮想サーバーにバインドされているサービスとサービスグループを表示するには

- 構成タブの左ペインで、**NetScaler > エンティティ > 仮想サーバー** をクリックします。
- 詳細ペインの で、バインドされているサービスとサービスグループを表示する仮想サーバーの名前をクリックし、 で または をクリックします。または、仮想サーバーの名前を右クリックし、 または をクリックします。



サービスのステータスを表示

サービスのリアルタイムの状態値と、サービスが現在の状態であった期間を監視できます。

仮想サーバーのステータスを表示するには

- 構成タブのナビゲーションペインで、**NetScaler > エンティティ > サービス** をクリックします。
- 詳細ペインの で、次の統計情報を表示します。
 - デバイス名 — サービスが構成されているデバイスの名前。
 - 名前 — サービスの名前。

- プロトコル — サービスの動作を決定するサービスの種類。例: HTTP、TCP、UDP、またはSSL。
 - 状態 — サービスの現在の状態。例: UP、DOWN、またはOUT OF SERVICE。
 - IPアドレス — サービスのIPアドレス。
 - ポート — サービスがリッスンするポート。
 - 最終状態変更 — サービスの最終状態変更からの経過時間（日、時間、分、秒）。つまり、サービスが現在の状態であった期間です。
- サービスがバインドされている仮想サーバーの表示

サービスがバインドされている仮想サーバーを表示し、仮想サーバーのリアルタイムステータスを監視できます。

サービスがバインドされている仮想サーバーを表示するには

- 構成タブで、ナビゲーションペインの**NetScaler > エンティティ > サービス**をクリックします。
- 詳細ペインの「サービス」で、バインドされている仮想サーバーを表示したいサービスの名前をクリックします。次に、メニューから **バインドされている仮想サーバー** を選択します。または、サービスを右クリックし、**バインドされている仮想サーバー** をクリックします。



サービスグループのステータスを表示する

SDXインターフェイスからサービスグループメンバーのリアルタイム状態を監視できます。

サービスグループのステータスを表示するには

- 「構成」タブのナビゲーションペインで、**NetScaler > エンティティ > サービスグループ**をクリックします。
- 詳細ペインの「サービスグループ」で、次の統計情報を表示します。
 - デバイス名 — サービスグループが構成されているデバイスの名前。
 - 名前 — サービスグループの名前。
 - IPアドレス — サービスグループのメンバーである各サービスのIPアドレス。
 - ポート — サービスグループのメンバーがリッスンするポート。
 - プロトコル — サービスグループの動作を決定するサービスタイプ。たとえば、HTTP、TCP、UDP、またはSSL。

- 有効な状態 — バックアップ仮想サーバーの状態に基づいて、仮想サーバーグループの有効な状態。たとえば、UP、DOWN、またはOUT OF SERVICE。
 - 状態 — サービスグループのメンバーの状態に基づいて、サービスグループの有効な状態。たとえば、UP、DOWN、またはOUT OF SERVICE。
 - 最終状態変更 — サービスグループメンバーの状態が最後に変更されてからの経過時間（日、時間、分、秒）。つまり、サービスグループメンバーが現在の状態であった期間。この情報は、NetScalerリリース9.0以降で構成されたサービスグループメンバーに対してのみ利用可能です。
- サービスがバインドされている仮想サーバーの表示

サービスがバインドされている仮想サーバーを表示し、仮想サーバーのリアルタイムステータスを監視できます。

サービスがバインドされている仮想サーバーを表示するには

- a. 「構成」タブの左ペインで、**NetScaler > エンティティ > サーバー**をクリックします。
- b. 右ペインの「サーバー」で、リストからサーバーを選択し、「アクション」メニューの「バインドされた仮想サービス」をクリックします。または、サービスを右クリックして「バインドされた仮想サーバー」をクリックします。

サーバーのステータスを表示する

NetScalerインスタンス全体のサーバーの状態を監視および管理できます。この監視により、サーバーのリアルタイムステータスが可視化され、多数のサーバーがある場合でもこれらのサーバーの管理が容易になります。

サーバーのステータスを表示するには

1. 構成タブのナビゲーションペインで、**NetScaler > エンティティ > サーバー**をクリックします。
2. 詳細ペインの「サーバー」で、次の統計情報を表示します。
 - デバイス名: サーバーが構成されているデバイスの名前を指定します。
 - 名前: サーバーの名前を指定します。
 - IPアドレス: サーバーのIPアドレスを指定します。クライアントはこのIPアドレスに接続要求を送信します。
 - 状態: サーバーの現在の状態を指定します。たとえば、UP、DOWN、OUT OF SERVICEなどです。

- 最終状態変更: サーバーの状態が最後に変更されてからの経過時間（日、時間、分、秒）を指定します。つまり、サーバーが現在の状態にある期間です。



ポーリング間隔を構成する

SDXアプライアンスが仮想サーバー、サービス、サービスグループ、およびサーバーのリアルタイム値をポーリングする時間間隔を設定できます。デフォルトでは、アプライアンスは30分ごとに値をポーリングします。

- 仮想サーバー、サービス、サービスグループ、およびサーバーのポーリング間隔を構成するには。
 - a. 構成タブで、**NetScaler > エンティティ**をクリックし、右ペインで「ポーリング間隔の構成」をクリックします。
 - b. 「ポーリング間隔の設定」ダイアログボックスで、SDXがエンティティ値をポーリングする時間間隔として設定したい分数を入力します。ポーリング間隔の最小値は30分です。「OK」をクリックします。

NetScalerインスタンスで生成されたイベントの監視と管理

イベント機能を使用して、NetScalerインスタンスで生成されたイベントを監視および管理します。管理サービスはイベントをリアルタイムで識別し、問題に即座に対処してNetScalerインスタンスを効果的に稼働させ続けるのに役立ちます。また、イベントルールを設定して、生成されたイベントをフィルタリングし、フィルタリングされたイベントリストに対してアクションを実行するための通知を受け取ることもできます。

すべてのイベントを表示する

NetScaler SDXアプライアンスにプロビジョニングされたNetScalerインスタンスで生成されたすべてのイベントを表示できます。各イベントの重大度、カテゴリ、日付、ソース、メッセージなどの詳細を表示できます。

イベントを表示するには、**Configuration > NetScaler > Events > All Events** に移動します。



イベントを選択して **Details** ボタンをクリックすると、イベント履歴とエンティティの詳細を表示できます。このページから特定のイベントを検索したり、削除したりすることもできます。

注: イベントを削除すると、復元することはできません。

- レポートの表示

レポートページには、イベントの概要がグラフィカルな形式で表示されます。レポートの表示は、さまざまな時間スケールに基づいて行うことができます。デフォルトでは、時間スケールは「日」です。

レポートを表示するには、**Configuration > NetScaler > Events > Reports** に移動します。管理サービスでサポートされているグラフィカルレポートは次のとおりです。

- イベント

イベントレポートは、イベント数を円グラフで表現したもので、重大度に基づいてセグメント化され、色分けされています。



特定の重大度のイベントの詳細を表示するには、円グラフのそのセグメントをクリックすると、次の詳細を表示できます。

- ソース: イベントが生成されたシステム名、ホスト名、またはIPアドレス。
- 日付: アラームが生成された日時。
- カテゴリ: イベントカテゴリ (例: `entityup`)。
- メッセージ: イベントの説明。

- すべてのイベント別上位10のNetScalerインスタンス

このレポートは、選択した時間スケールでのイベント数に基づいて、上位10のNetScalerインスタンスを表示する棒グラフです。



- エンティティ状態変更イベント別上位10のNetScalerインスタンス

このレポートは、選択した時間スケールでのエンティティ状態変更の数に基づいて、上位10のNetScalerインスタンスを表示する棒グラフです。エンティティの状態変更は、エンティティの稼働、エンティティの停止、またはサービス停止イベントを反映します。



- しきい値違反イベント別上位10のNetScalerインスタンス

このレポートは、選択した時間スケールでのしきい値違反イベントの数に基づいて、上位10のNetScalerインスタンスを表示する棒グラフです。しきい値違反イベントは、次のイベントを反映します。

- cpuUtilization
- memoryUtilization
- diskUsageHigh
- temperatureHigh
- voltageLow
- voltageHigh
- fanSpeedLow
- temperatureCpuHigh
- interfaceThroughputLow
- interfaceBWUseHigh
- aggregateBWUseHigh
- **ハードウェア障害イベントによるNetScalerインスタンス上位10件** このレポートは、選択した時間スケールにおけるハードウェア障害イベントの数に基づいて、上位10件のNetScalerインスタンスを表示する棒グラフです。ハードウェア障害イベントには、次のイベントが含まれます。

- hardDiskDriveErrors
- compactFlashErrors
- powerSupplyFailed
- "sslCardFailed"

- **構成変更イベントによるNetScalerインスタンス上位10件**

このレポートは、選択した時間スケールにおける構成変更イベントの数に基づいて、上位10件のNetScalerインスタンスを反映する棒グラフです。グラフをクリックすると、インスタンスのユーザーベースの構成変更をドリルダウンして表示できます。このグラフをクリックすると、承認および実行ステータスの詳細をさらに表示できます。

- **<認証失敗イベントによるNetScalerインスタンス上位10件**

このレポートは、選択した時間スケールにおける認証失敗イベントの数に基づいて、上位10のNetScalerインスタンスを表示する棒グラフです。グラフをクリックすると、インスタンスのユーザーベースの認証失敗の詳細を表示できます。



- イベントルールの構成

特定の条件を持つルールを構成し、そのルールにアクションを割り当てることで、一連のイベントをフィルタリングできます。生成されたイベントがルールのフィルタ条件を満たすと、そのルールに関連付けられたアクションが実行されます。フィルタを作成できる条件は、重大度、デバイス、失敗オブジェクト、カテゴリです。

イベントに次のアクションを割り当てることができます。

- **電子メール送信アクション** フィルタ条件に一致するイベントに対して電子メールを送信します。
- **SMS送信アクション** フィルタ条件に一致するイベントに対してショートメッセージサービス (SMS) を送信します。

イベントルールを追加するには

- a. **構成 > NetScaler > イベント > イベントルール** に移動し、 をクリックします。
- b. ページで、次のパラメータを設定します。

- **名前**—イベントルールの名前。
- **有効**—イベントルールを有効にします。
- **重大度**—イベントルールを追加するイベントの重大度。
- **デバイス**—イベントルールを定義するNetScalerインスタンスのIPアドレス。
- **カテゴリ** — NetScalerインスタンスによって生成されたイベントのカテゴリ。
- **障害オブジェクト** — イベントが生成されたエンティティインスタンスまたはカウンター。



注: このリストには、すべてのしきい値関連イベントのカウンター名、すべてのエンティティ関連イベントのエンティティ名、および証明書関連イベントの証明書名を含めることができます。

- c. をクリックします。
- d. で、イベントの通知アクションを割り当てることができます。
 - a. **メールプロファイル** — メールサーバーとメールプロファイルの詳細。イベントが定義されたフィルター条件を満たした場合に、メールがトリガーされます。
 - b. **SMSプロファイル** — SMSサーバーとSMSプロファイルの詳細。イベントが定義されたフィルター条件を満たした場合に、SMSがトリガーされます。



e. をクリックします。

- イベントの構成

SDXアプライアンス上のNetScalerインスタンスに対して生成されるイベントに、重大度レベルを割り当てることができます。次の種類の重大度レベルを定義できます: 重大、メジャー、マイナー、警告、クリア、情報。特定の期間、イベントを抑制することもできます。重大度を構成するには:

a. >>> に移動し、リストからイベントを選択して、 をクリックします。



b. ページで、ドロップダウンリストから必要な重大度レベルを選択します。

c. あるいは、チェックボックスを選択することでイベントを抑制できます。また、オプションを使用して、このイベントを抑制したい NetScaler インスタンスを指定することもできます。



d. をクリックします。

SDXアプライアンス上のNetScalerインスタンスに対するCall Homeサポート

Call Home機能は、一般的なエラー状態についてNetScalerインスタンスを監視します。

Management Serviceユーザーインターフェイスから、NetScalerインスタンスでCall Home機能を構成、有効化、または無効化できるようになりました。

注： アプライアンスで事前定義されたエラー状態が発生した場合にCall Homeがシステムデータをサーバーにアップロードできるようにするには、NetScalerインスタンスをCitrixテクニカルサポートサーバーに登録する必要があります。NetScalerインスタンスでCall Home機能を有効にすると、登録プロセスが開始されます。

- NetScalerインスタンスでのCall Homeの有効化と無効化

Management ServiceからNetScalerインスタンスでCall Home機能を有効にできます。Call Home機能を有効にすると、Call HomeプロセスによってNetScalerインスタンスがCitrixテクニカルサポートサーバーに登録されます。登録が完了するまでに時間がかかります。その間、Management Serviceは登録の進行状況を表示します。

Call Home機能を有効にするには、**Configuration > NetScaler > Call Home**に移動し、NetScalerインスタンスを選択して、Enableボタンをクリックします。確認ページで、Yesをクリックします。

Call Home機能を無効にするには、**Configuration > NetScaler > Call Home**に移動し、NetScalerインスタンスを選択して、Disableボタンをクリックします。確認ページで、Yesをクリックします。

Call Homeを有効にした場合、次のオプションを構成できます。

- a. (オプション) 管理者のメールアドレスを指定します。Call Homeプロセスは、メールアドレスをサポートサーバーに送信し、Call Homeに関する今後の連絡のために保存されます。
 - b. (オプション) Call Homeプロキシモードを有効にします。Call Homeは、プロキシサーバーを介してNetScalerインスタンスのデータをCitrix TaaSサーバーにアップロードできます。この機能を使用するには、NetScalerインスタンスでこれを有効にし、HTTPプロキシサーバーのIPアドレスとポート番号を指定します。プロキシサーバーからTaaSサーバー（インターネット経由）へのすべてのトラフィックはSSL経由で暗号化されるため、データセキュリティとプライバシーが損なわれることはありません。
- Management ServiceからNetScalerインスタンスでCall Homeを構成するには

Call Home機能は、単一のインスタンスまたは複数のインスタンスで同時に構成できます。

単一のNetScalerインスタンスでCall Home機能を構成するには、**Configuration > NetScaler > Call Home**に移動し、NetScalerインスタンスを選択して、Configureボタンをクリックします。Configure Call Homeページで、OKをクリックします。



複数のNetScalerインスタンスでCall Home機能を構成するには、**Configuration > NetScaler**に移動します。右側のペインで、Call Homeをクリックします。Configure Call Homeページで、Available InstancesセクションからNetScalerインスタンスを選択し、その他の詳細を指定して、OKをクリックします。



- NetScalerインスタンスのポーリング

すべてのNetScalerインスタンスからCall Home機能をポーリングし、現在のステータスを表示するには、**Configuration > NetScaler > Call Home**に移動し、**Poll Now**をクリックします。確認ページで、**Yes**をクリックします。

システムヘルス監視

システムヘルス監視は、監視対象コンポーネントのエラーを検出し、障害を回避するための是正措置を講じられるようにします。NetScaler SDXアプライアンスでは、以下のコンポーネントが監視されます。

- ハードウェアおよびソフトウェアリソース
- 物理ディスクと仮想ディスク
- ファン、温度、電圧、電源センサーなどのハードウェアセンサー
- インターフェイス

タブで、をクリックします。すべてのコンポーネントの概要が表示されます。監視対象コンポーネントの詳細を表示するには、を展開し、監視するコンポーネントをクリックします。

- SDXアプライアンスのリソースの監視

SDXアプライアンスのハードウェアおよびソフトウェアコンポーネントを監視し、必要に応じて是正措置を講じることができます。監視対象コンポーネントを表示するには、タブでを展開し、をクリックします。ハードウェアおよびソフトウェアリソースの詳細が表示されます。すべてのハードウェアコンポーネントについて、現在値と期待値が表示されます。BMCファームウェアバージョンを除くソフトウェアコンポーネントについては、現在値と期待値は「該当なし (NA)」と表示されます。

- **名前:** CPU、メモリ、BMCファームウェアバージョンなどのコンポーネントの名前。
- **ステータス:** コンポーネントの状態（条件）。ハードウェアおよびBMCファームウェアバージョンでは、ERRORは期待値からの逸脱を示します。Citrix Hypervisor™への呼び出しの場合、ERRORは管理サービスがAPI、HTTP、PING、またはSSH呼び出しを使用してCitrix Hypervisorと通信できないことを示します。ヘルスマニタープラグインの場合、ERRORはプラグインがCitrix Hypervisorにインストールされていないことを示します。
- **現在値:** コンポーネントの現在値。通常の状態では、現在値は期待値と同じです。
- **期待値:** コンポーネントの期待値。Citrix Hypervisorへのソフトウェア呼び出しには適用されません。

SDXアプライアンスのストレージリソースを監視する

SDXアプライアンスのディスクを監視し、必要に応じて是正措置を講じることができます。監視対象コンポーネントを表示するには、タブでを展開し、をクリックします。物理ディスク、および物理ディスクから作成された仮想ディスクまたはパーティションの詳細が表示されます。

ディスク (Disk) については、次の詳細が表示されます。

- **名前** 物理ディスクの名前。
- **サイズ**: ディスクのサイズ (GB)。
- **使用済み**: ディスク上のデータ量 (GB)。
- **トランザクション/秒**: 1秒あたりに読み書きされるブロック数。この数値は `iostat` 出力から読み取られます。
- **読み取りブロック/秒**: 1秒あたりに読み取られるブロック数。この値を使用して、ディスクからの出力レートを測定できます。
- **書き込みブロック/秒**: 1秒あたりに書き込まれるブロック数。この値を使用して、ディスクへの入力レートを測定できます。
- **総読み取りブロック数**: アプライアンスが最後に起動されてから読み取られたブロック数。
- **総書き込みブロック数**: アプライアンスが最後に起動されてから書き込まれたブロック数。

仮想ディスクまたはパーティション (Storage Repository) については、次の詳細が表示されます。

- **ドライブベイ**: ドライブベイ内のドライブの番号。このパラメータでデータをソートできます。
- **ステータス**: ドライブベイ内のドライブの状態 (コンディション)。可能な値:
 - GOOD: ドライブは良好な状態であり、使用可能です。
 - FAIL: ドライブが故障しており、交換する必要があります。
 - MISSING: ドライブベイでドライブが検出されません。
 - 不明: ドライブベイに新しい未フォーマットのドライブが存在します。
- **名前**: ストレージリポジトリのシステム定義名。
- **サイズ**: ストレージリポジトリのサイズ (GB単位)。
- **使用済み**: ストレージリポジトリ内のデータ量 (GB単位)。

SDXアプライアンスのハードウェアセンサーを監視する

SDXアプライアンスのハードウェアコンポーネントを監視し、必要に応じて是正措置を講じることができます。監視タブで、システムヘルスを展開し、ハードウェアセンサーをクリックします。監視機能は、さまざまなファンの速度、さまざまなコンポーネントの温度と電圧、および電源の状態に関する詳細を表示します。

ファン速度については、次の詳細が表示されます。

- **名前**: ファンの名前。

- **ステータス:** ファンの状態。ERRORは、期待値からの逸脱を示します。NAは、ファンが存在しないことを示します。
- **現在の値 (RPM):** 現在の1分あたりの回転数。

温度情報には、次の詳細が含まれます。

- **名前:** CPUやメモリモジュールなどのコンポーネントの名前 (例: P1-DIMM1A)。
- **ステータス:** コンポーネントの状態。ERRORは、現在の値が範囲外であることを示します。
- **現在の値 (摂氏):** コンポーネントの現在の温度 (摂氏)。

電圧情報には、次の詳細が含まれます。

- **名前:** CPUコアなど、コンポーネントの名前。
- **ステータス:** コンポーネントの状態。ERRORは、現在の値が範囲外であることを示します。
- **現在の値 (ボルト):** コンポーネントに存在する現在の電圧。

電源に関する情報には、次の詳細が含まれます。

- **名前:** コンポーネントの名前。
- **ステータス:** コンポーネントの状態。可能な値:
 - **エラー:** 電源が1つしか接続されていないか、動作していません。
 - **OK:** 両方の電源が接続されており、期待どおりに動作しています。

SDXアプライアンスのインターフェースを監視する

SDXアプライアンスのインターフェースを監視し、必要に応じて是正措置を講じることが出来ます。 **Monitoring** タブで、 **System Health** を展開し、 **Interfaces** をクリックします。監視機能は、各インターフェースに関する次の情報を詳細に示します。

- **インターフェース:** SDXアプライアンス上のインターフェース番号。
- **ステータス:** インターフェースの状態。可能な値: UP、DOWN。
- **割り当て済みVF/合計:** インターフェースに割り当てられている仮想機能 (VF) の数、およびそのインターフェースで利用可能な仮想機能の数。プラットフォームによってサポートされるVFの数は異なります。
- **送信パケット:** アプライアンスが最後に起動されてから送信されたパケットの数。
- **受信パケット:** アプライアンスが最後に起動されてから受信されたパケットの数。
- **Tx バイト:** アプライアンスが最後に起動されてから送信されたバイト数。

- **Rx バイト:** アプライアンスが最後に起動してから受信されたバイト数。
- **Tx エラー:** アプライアンスが最後に起動してからデータ送信中に発生したエラー数。
- **Rx エラー:** アプライアンスが最後に起動してからデータ受信中に発生したエラー数。

システム通知設定の構成

システム関連のさまざまな機能について、特定のユーザーグループと通信するために通知を送信できます。SDX Management Service で通知サーバーを設定し、電子メールおよびショートメッセージサービス (SMS) ゲートウェイサーバーを構成して、ユーザーに電子メールおよびテキスト (SMS) 通知を送信できます。

注

SDX Management Service リリース 11.1 にアップグレードすると、すべてのイベントカテゴリでシステム通知が有効になり、通知は既存の電子メールまたはSMSプロファイルに送信されます。

システム通知設定を構成するには

1. システム > 通知 > 設定 に移動し、**通知設定の変更** をクリックします。
2. In the **Configure System Notification Settings** page, enter the following details: - **カテゴリ** – SDX Management Service によって生成されるイベントのカテゴリ。 - **電子メール** – ドロップダウンメニューから電子メール配布リストを選択します。+ アイコンをクリックし、適切なフィールドに新しい電子メールサーバーの詳細を入力して、新しい電子メール配布リストを作成することもできます。 - **SMS (テキストメッセージ)** – ドロップダウンメニューからSMS配布リストを選択します。また、作成することもできます。新しいSMS配布リストは、+ アイコンをクリックし、適切なフィールドに新しいSMSサーバーの詳細を入力して作成します。
3. **OK** をクリックします。

マネジメントサービスから機能を有効/無効にする

注

この機能は、リリース 13.1 ビルド 12.x 以降で利用可能です。

NetScaler SDX アプライアンスでは、Management Service は、SSL 証明書、ネットワーク機能、構成監査などの操作のために、バックグラウンドで NetScaler インスタンスをポーリングします。要件に応じて、このポーリングを有効または無効にするオプションがあります。このポーリングを無効にすると、Management Service と ADC インスタンスのパフォーマンスが向上します。

GUI を使用して機能を有効または無効にするには

1. **System > System Settings** に移動します。
2. **Configure Features** をクリックします。
3. 機能を選択し、**Enable** または **Disable** をクリックします。

管理サービスを設定する

管理サービスを使用すると、クライアントセッションを管理し、要件に応じてユーザーアカウントの作成と管理、バックアップおよびプルーニングポリシーの調整などの構成タスクを実行できます。また、管理サービスを再起動したり、管理サービスのバージョンをアップグレードしたりすることもできます。さらに、管理サービスとCitrix Hypervisor™のtarファイルを作成し、テクニカルサポートに送信することもできます。

クライアントセッションを管理する

ユーザーが管理サービスにログオンすると、クライアントセッションが作成されます。アプライアンス上のすべてのクライアントセッションは、**セッションペイン**で表示できます。

セッションペインでは、次の詳細を表示できます。

- **ユーザー名:** セッションに使用されているユーザーアカウント。
- **IPアドレス:** セッションが作成されたクライアントのIPアドレス。
- **ポート:** セッションに使用されているポート。
- **ログイン時刻:** SDXアプライアンスで現在のセッションが作成された時刻。
- **最終アクティビティ時刻:** セッションでユーザーアクティビティが最後に検出された時刻。
- **セッション有効期限:** セッションの有効期限が切れるまでの残り時間。

クライアントセッションを表示するには、**構成**タブで、**システム > セッション**に移動します。

クライアントセッションを終了するには、**セッションペイン**で、削除したいセッションをクリックし、**セッションの終了**をクリックします。

セッションを開始したクライアントから、そのセッションを終了することはできません。

ポリシーを設定する

ログデータのサイズを管理可能な範囲に保つため、SDXアプライアンスは指定された時間にバックアップおよびデータプルーニングポリシーを自動的に実行します。

プルーニングポリシーは毎日午前0時00分に行われ、アプライアンスに保持するデータの期間（日数）を指定します。デフォルトでは、アプライアンスは3日より古いデータをプルーニングし

ますが、保持したいデータの期間（日数）を指定できます。イベントログ、監査ログ、タスクログのみがプルーニングされます。

バックアップポリシーは毎日午前0時30分には実行され、ログと構成ファイルのバックアップを作成します。デフォルトでは、ポリシーは3つのバックアップを保持しますが、保持したいバックアップの数を指定できます。また、バックアップポリシーを使用して、次のことができます。

- バックアップファイルを暗号化します。
- FTP、SFTP、およびSCPを使用して、バックアップファイルを外部バックアップサーバーに転送するようにSDXアプライアンスを設定します。

ログデータがプルーニングされる日数を指定するには：

1. **Configuration**タブのナビゲーションペインで、**System**をクリックします。
2. **System**ペインの**Policy Administration**の下にある**Prune Policy**をクリックします。
3. **Modify Prune Policy**ダイアログボックスの****Data to keep (days)****に、アプライアンスが常に保持する必要があるデータの期間（日数）を指定します。
4. **OK**をクリックします。

バックアップポリシーを設定するには：

1. **Configuration**タブのナビゲーションペインで、**System**をクリックします。
2. **System**ペインの**Policy Administration**の下にある**Backup Policy**をクリックします。
3. **Modify Backup Policy**ダイアログボックスの**Previous Backups to retain**に、アプライアンスが常に保持する必要があるバックアップの数を指定します。
4. **Encrypt Backup File**を選択して、バックアップファイルを暗号化します。
5. 「**外部転送**」を選択し、バックアップファイルを外部バックアップサーバーに転送するために、次の操作を行います。
 - a. 「**サーバー**」フィールドに、外部バックアップサーバーのホスト名またはIPアドレスを入力します。
 - b. 「**ユーザー名**」フィールドと「**パスワード**」フィールドに、外部バックアップサーバーにアクセスするためのユーザー名とパスワードを入力します。
 - c. 「**ポート**」フィールドに、ポート番号を入力します。
 - d. 「**転送プロトコル**」フィールドで、バックアップファイルを外部バックアップサーバーに転送するために使用するプロトコルを選択します。

- e. 「ディレクトリパス」フィールドに、バックアップファイルを保存する外部バックアップサーバー上のディレクトリのパスを入力します。
6. 「転送後に管理サービスからファイルを削除」：バックアップファイルを外部バックアップサーバーに転送した後、SDXアプライアンスからバックアップファイルを削除する場合は、これを選択します。
7. 「OK」をクリックします。

管理サービスを再起動する

「システム」ペインから管理サービスを再起動できます。管理サービスを再起動しても、インスタンスの動作には影響しません。管理サービスの再起動プロセス中も、インスタンスは機能し続けます。

管理サービスを再起動するには：

1. 「構成」タブのナビゲーションペインで、「システム」をクリックします。
2. 「システム」ペインの「システム管理」で、「管理サービスの再起動」をクリックします。

管理サービスファイルを削除する

不要な管理サービスのビルドファイルとドキュメントファイルをSDXアプライアンスから削除できます。

Management Serviceファイルを削除するには：

1. 構成タブのナビゲーションペインで、**Management Service**を展開し、削除するファイルをクリックします。
2. 詳細ペインで、ファイル名を選択し、**削除**をクリックします。

テクニカルサポート用のtarアーカイブを生成する

テクニカルサポートオプションを使用して、Citrix®テクニカルサポートに提出するためのデータと統計のtarアーカイブを生成できます。このtarは、Management ServiceまたはCitrix Hypervisor、あるいはその両方に対して同時に生成できます。その後、ファイルをローカルシステムにダウンロードして、Citrixテクニカルサポートに送信できます。

テクニカルサポートペインで、次の詳細を表示できます。

- **名前:** tarアーカイブファイルの名前。ファイル名には、tarがManagement Service用かCitrix Hypervisorサーバー用かが示されます。
- **最終変更日時:** このファイルが最後に変更された日付。
- **サイズ:** tarファイルのサイズ。

テクニカルサポート用のtarアーカイブを生成するには：

1. **構成**タブで、**診断 > テクニカルサポート**の順に移動します。
2. **詳細**ペインで、**アクション**リストから**テクニカルサポートファイルの生成**を選択します。
3. **テクニカルサポートファイルの生成**ダイアログボックスで、**モード**リストから適切なオプションを選択します。
4. **OK**をクリックします。

テクニカルサポート用のtarアーカイブをダウンロードするには：

1. 「**Technical Support**」ペインで、ダウンロードするテクニカルサポートファイルを選択します。
2. 「**Action**」リストから「**Download**」を選択します。ファイルはローカルコンピュータに保存されます。

Management ServiceのCLIサポート

CLIを使用してManagement Serviceに対する操作を実行できるようになりました。以下の操作がサポートされています。

- **Add、Set、Delete** — リソースを構成するため。
- **Do** — システムレベルの操作を実行するため。例えば、管理サービスのアップグレード、シャットダウン、または再起動など。
- **Save** — プロビジョニングに使用されるインターフェースを追加するため。

CLIにアクセスするには、Management ServiceのIPアドレスに接続されている任意のワークステーションからセキュアシェル (SSH) クライアントを起動します。管理者資格情報を使用してログインします。

コマンドの使用法と構文に関する詳細情報は、manページからアクセスできます。

注: CLIはコンソールアクセスではサポートされていません。

認証および承認設定の構成

NetScaler SDX Management Service の認証は、ローカルまたは外部で行うことができます。外部認証の場合、Management Service は外部サーバーからの応答に基づいてユーザーアクセスを許可します。Management Service は、次の外部認証プロトコルをサポートしています。

- リモート認証ダイヤルインユーザーサービス (RADIUS)
- ターミナルアクセスコントローラアクセス制御システム (TACACS)
- 軽量ディレクトリアクセスプロトコル (LDAP)

Management Service は、SSH からの認証要求もサポートしています。SSH 認証は、キーボードインタラクティブ認証要求のみをサポートします。SSH ユーザーの承認は、管理者権限のみに制限されています。読み取り専用権限を持つユーザーは、SSH を介してログオンできません。

認証を構成するには、認証タイプを指定し、認証サーバーを構成します。

Management Service を介した承認はローカルです。Management Service は、2 つのレベルの承認をサポートしています。管理者権限を持つユーザーは、管理サービスに対してあらゆるアクションを実行できます。読み取り専用権限を持つユーザーは、読み取り操作のみを実行できます。SSH ユーザーの承認は、管理者権限のみに制限されています。読み取り専用権限を持つユーザーは、SSH を介してログオンできません。

RADIUS および LDAP の承認は、グループ抽出によってサポートされます。Management Service で RADIUS または LDAP サーバーを構成する際に、グループ抽出属性を設定できます。抽出されたグループ名は、Management Service 上のグループ名と照合され、ユーザーに与えられる権限が決定されます。ユーザーは複数のグループに属することができます。その場合、ユーザーが属するいずれかのグループに管理者権限がある場合、ユーザーは管理者権限を持ちます。構成中にデフォルト認証グループ属性を設定できます。このグループは、承認のために抽出されたグループとともに考慮されます。

TACACS認証では、TACACSサーバー管理者は、管理者権限を持つユーザーには特別なコマンド admin を許可し、読み取り専用権限を持つユーザーにはこのコマンドを拒否する必要があります。ユーザーがSDXアプライアンスにログオンすると、Management Serviceは、ユーザーがこのコマンドを実行する権限があるかどうかを確認します。ユーザーに権限がある場合、ユーザーには管理者権限が割り当てられ、そうでない場合、ユーザーには読み取り専用権限が割り当てられません。

ユーザーグループの追加

グループとは、共通の情報にアクセスしたり、同様の種類のタスクを実行したりする必要があるユーザーの論理的なセットです。共通の操作のセットによって定義されたグループにユーザーを編成できます。個々のユーザーではなくグループに特定の権限を付与することで、ユーザー作成時の時間を節約できます。

外部認証サーバーを認証に使用している場合、SDX のグループは、認証サーバーで構成されたグループと一致するように構成できます。認証サーバー上のグループと名前が一致するグループに属するユーザーがログオンして認証されると、そのユーザーはグループの設定を継承します。

ユーザーグループを追加するには

1. **Configuration** タブで、**System** の下の **User Administration** を展開し、**Groups** をクリックします。
2. 詳細ペインで、**追加** をクリックします。



3. **システムグループの作成** ページで、次のパラメータを設定します。

- グループ名
- グループの説明
- システムアクセス: このチェックボックスをオンにすると、SDXアプライアンス全体と、その上で実行されているインスタンスへのアクセスが許可されます。または、インスタンスレベルのアクセスの場合、**インスタンス**の下でインスタンスを指定します。
- 権限
- ユーザーセッションタイムアウトの設定
- ユーザー: グループに属するデータベースユーザー。グループに追加するユーザーを選択します。

4. **作成と閉じる** をクリックします。

注: バージョン10.5からバージョン11.1にアップグレードされたSDXアプライアンスで管理者ロールを持つグループを作成するには、「読み取り/書き込み」権限と「システムアクセス」チェックボックスを選択します。SDX 10.5では、このチェックボックスは利用できず、権限の値は「管理者」と「読み取り専用」です。

ユーザーアカウントの設定

ユーザーは、アプライアンス管理タスクを実行するためにSDXアプライアンスにログオンします。ユーザーがアプライアンスにアクセスできるようにするには、そのユーザーのユーザーアカウントをSDXアプライアンス上に作成する必要があります。ユーザーはアプライアンス上でローカルに認証されます。

重要: パスワードは、SDXアプライアンス、Management Service、およびCitrix Hypervisorに適用されます。Citrix Hypervisor上で直接パスワードを変更しないでください。

ユーザーアカウントを設定するには

1. 「**Configuration**」タブで、「**System**」の下にある「**Administration**」を展開し、「**Users**」をクリックします。「**Users**」ペインに、既存のユーザーアカウントとその権限のリストが表示されます。
2. 「**Users**」ペインで、次のいずれかを実行します。
 - ユーザーアカウントを作成するには、「**Add**」をクリックします。
 - ユーザーアカウントを変更するには、ユーザーを選択し、「**Modify**」をクリックします。
3. 「**Create System User**」または「**Modify System User**」ダイアログボックスで、次のパラメータを設定します。
 - 名前*—アカウントのユーザー名。名前に使用できる文字は、a～z、A～Zの文字、0～9の数字、ピリオド（.）、スペース、アンダースコア（_）です。最大長：128。名前は変更できません。
 - パスワード*—アプライアンスにログオンするためのパスワード。最大長：128
 - パスワードの確認*—パスワード。
 - 権限*—アプライアンスでのユーザーの特権。指定可能な値：
 - admin—ユーザーは、Management Serviceに関連するすべての管理タスクを実行できます。
 - read-only—ユーザーはシステムを監視し、アカウントのパスワードを変更することのみができます。デフォルト：admin。
 - 外部認証を有効にする—このユーザーの外部認証を有効にします。Management Serviceは、データベースユーザー認証の前に外部認証を試行します。このパラメータが無効になっている場合、ユーザーは外部認証サーバーで認証されません。注：リモート認証サーバーに到達できない場合、ユーザーはアプライアンスへのアクセスを失う可能性があります。

す。そのような場合、認証はデフォルトのadminユーザー（`nsroot`）にフォールバックします。

- セッションタイムアウトの構成—ユーザーがアクティブな状態を維持できる期間を構成できます。次の詳細を指定します。
 - セッションタイムアウト—ユーザーセッションがアクティブな状態を維持できる期間。
 - セッションタイムアウト単位—タイムアウト単位（分または時間）。
- グループ—ユーザーにグループを割り当てます。

*必須パラメーター

4. 「作成」または「OK」をクリックし、次に「閉じる」をクリックします。作成したユーザーは「ユーザー」ペインに表示されます。

ユーザーアカウントを削除するには

1. 構成タブのナビゲーションペインで、システムを展開し、管理を展開して、ユーザーをクリックします。
2. ユーザーペインで、ユーザーアカウントを選択し、削除をクリックします。
3. 確認メッセージボックスで、OKをクリックします。

認証タイプを設定する

Management Serviceインターフェースから、ローカル認証または外部認証を指定できます。外部認証は、デフォルトではローカルユーザーに対して無効になっています。ローカルユーザーを追加するとき、またはユーザーの設定を変更するときに、「外部認証を有効にする」オプションをオンにすることで有効にできます。

重要: 外部認証は、RADIUS、LDAP、またはTACACS認証サーバーを設定した後にのみサポートされます。

認証タイプを設定するには

1. 構成タブの「システム」の下で、「認証」をクリックします。
2. 詳細ペインで、「認証構成」をクリックします。
3. 次のパラメーターを設定します。
 - サーバータイプ—ユーザー認証用に構成された認証サーバーのタイプ。可能な値：LDAP、RADIUS、TACACS、およびローカル。

- サーバー名 — Management Serviceで構成された認証サーバーの名前です。メニューには、選択した認証タイプ用に構成されたすべてのサーバーが表示されます。
- フォールバックローカル認証を有効にする — あるいは、外部認証が失敗した場合に、ローカル認証でユーザーを認証することもできます。このオプションはデフォルトで有効になっています。

4. OKをクリックします。

基本認証を有効または無効にする

基本認証を使用して、Management Service NITROインターフェイスに認証できます。リリース13.1ビルド59.x以降、**基本認証を許可**オプションはデフォルトで無効になっています。

Management Serviceインターフェイスを使用して基本認証を有効または無効にするには、次の手順を実行します。

1. **構成**タブで、**システム**をクリックします。
2. **システム設定グループ**で、**システム設定の変更**をクリックします。
3. システム設定の構成ダイアログボックスで、**基本認証を許可**を選択して有効にするか、**基本認証を許可**をクリアして無効にします。
4. **OK**をクリックします。

外部認証サーバーの構成

NetScaler SDX Management Serviceは、ローカルユーザーアカウントまたは外部認証サーバーを使用してユーザーを認証できます。アプライアンスは次の認証タイプをサポートしています。

- ローカル — 外部認証サーバーを参照せずに、パスワードを使用してManagement Serviceに認証します。ユーザーデータはManagement Serviceにローカルに保存されます。
- RADIUS — 外部RADIUS認証サーバーに対して認証します。
- LDAP — 外部LDAP認証サーバーに対して認証します。
- TACACS — 外部のTerminal Access Controller Access-Control System (TACACS) 認証サーバーに対して認証します。

外部認証を構成するには、認証タイプを指定し、認証サーバーを構成します。

RADIUSサーバーの追加

RADIUS認証を構成するには、認証タイプをRADIUSとして指定し、RADIUS認証サーバーを構成します。

Management Serviceは、RADIUS仕様に従ってRADIUSチャレンジレスポンス認証をサポートしています。RADIUSユーザーは、RADIUSサーバーでワンタイムパスワードを設定できます。ユーザーがSDXアプライアンスにログオンすると、このワンタイムパスワードを指定するように求められます。

RADIUSサーバーを追加するには

1. **Configuration** タブで、**System** の下にある **Authentication** を展開し、**Radius** をクリックします。
2. 詳細ペインで、**Add** をクリックします。
3. **Create Radius Server** ダイアログボックスで、パラメーターの値を入力または選択します。
 - 名前* — サーバーの名前。
 - サーバー名 / IPアドレス* — 完全修飾ドメイン名 (FQDN) またはサーバーIPアドレス。注: DNSは指定されたFQDNをIPアドレスに解決できる必要があります、FQDNの解決にはプライマリDNSのみが使用されます。プライマリDNSを手動で設定するには、「FQDN名前解決のためのプライマリDNSの追加」セクションを参照してください。
 - ポート* — RADIUSサーバーが稼働しているポート。デフォルト値: 1812。
 - タイムアウト* — システムがRADIUSサーバーからの応答を待機する秒数。デフォルト値: 3。
 - シークレットキー* — クライアントとサーバー間で共有されるキー。この情報は、システムとRADIUSサーバー間の通信に必要です。
 - NAS IPアドレス抽出を有効にする — 有効にすると、RADIUSプロトコルに従って、管理サービスIPアドレスが `nasip` としてサーバーに送信されます。
 - NASID — 設定されている場合、この文字列はRADIUSプロトコルに従って `nasid` としてRADIUSサーバーに送信されます。
 - グループプレフィックス — RADIUSグループ抽出のために、RADIUS属性内のグループ名の前に付加されるプレフィックス文字列。
 - グループベンダーID — RADIUSグループ抽出を使用するためのベンダーID。
 - グループ属性タイプ — RADIUSグループ抽出のための属性タイプ。
 - グループセパレーター — RADIUSグループ抽出のために、RADIUS属性内のグループ名を区切るグループセパレーター文字列。
 - IPアドレスベンダー識別子 — イントラネットIPを示すRADIUS内の属性のベンダーID。値が0の場合、属性はベンダーエンコードされていないことを示します。
 - IPアドレス属性タイプ — RADIUS応答におけるリモートIPアドレス属性の属性タイプ。

- パスワードベンダー識別子—RADIUS応答におけるパスワードのベンダーID。ユーザーパスワードを抽出するために使用されます。
- パスワード属性タイプ—RADIUS応答におけるパスワード属性の属性タイプ。
- パスワードエンコーディング—システムからRADIUSサーバーへ送信されるRADIUSパケット内でパスワードがどのようにエンコードされるべきか。指定可能な値: pap、chap、mschapv1、および mschapv2。
- デフォルト認証グループ—抽出されたグループに加えて、認証が成功したときに選択されるデフォルトグループ。
- アカウンティング—Management ServiceがRADIUSサーバーで監査情報をログに記録できるようにします。

4. 作成をクリックし、次に閉じるをクリックします。

LDAP認証サーバーの追加

LDAP認証を設定するには、認証タイプをLDAPとして指定し、LDAP認証サーバーを設定します。

LDAPサーバーを追加するには

1. 「構成」タブの「システム」で、「認証」を展開し、「LDAP」をクリックします。
2. 詳細ペインで、「追加」をクリックします。
3. 「LDAPサーバーの作成」ダイアログボックスで、パラメーターの値を入力または選択します。
 - 名前*—サーバーの名前。
 - サーバー名 / IPアドレス*—FQDNまたはサーバーIPアドレス。注: DNSは指定されたFQDNをIPアドレスに解決できる必要があります、プライマリDNSのみがFQDNの解決に使用されます。プライマリDNSを手動で設定するには、「FQDN名前解決のためのプライマリDNSの追加」セクションを参照してください。
 - ポート*—LDAPサーバーが実行されているポート。デフォルト値: 389。
 - タイムアウト*—システムがLDAPサーバーからの応答を待機する秒数。
 - ベースDN—LDAP検索を開始する必要があるベース、またはノード。
 - タイプ—LDAPサーバーのタイプ。可能な値: Active Directory (AD)およびNovell Directory Service (NDS)。
 - 管理バインドDN — LDAPサーバーへのバインドに使用される完全な識別名。
 - 管理パスワード — LDAPサーバーへのバインドに使用されるパスワード。

- LDAP証明書の検証 — LDAPサーバーから受信した証明書を検証するには、このオプションをオンにします。
- LDAPホスト名 — LDAPサーバーのホスト名。validateServerCertパラメータが有効になっている場合、このパラメータはLDAPサーバーからの証明書上のホスト名を指定します。ホスト名が一致しない場合、接続エラーが発生します。
- サーバーログオン名属性 — 外部LDAPサーバーまたはActive Directoryを照会するためにシステムが使用する名前属性。
- 検索フィルター — デフォルトのLDAPユーザー検索文字列と組み合わせて値を形成する文字列。たとえば、ldaploginame `samaccount` とユーザーが指定したユーザー名 bob を使用して vpnallowed=true とすると、LDAP検索文字列は (&(vpnallowed=true)(samaccount=bob)) になります。
- グループ属性 — LDAPサーバーからのグループ抽出に使用する属性名。
- サブ属性名 — LDAPサーバーからのグループ抽出に使用するサブ属性名。
- セキュリティタイプ — アプライアンスと認証サーバー間の通信に使用する暗号化のタイプ。可能な値:

PLAINTEXT: 暗号化は不要です。

TLS: TLSプロトコルを使用して通信します。

SSL: SSLプロトコルを使用して通信します。

- デフォルト認証グループ — 認証が成功した場合に、抽出されたグループに加えて選択されるデフォルトのグループ。
- リフェラル — LDAPサーバーから受信したLDAPリフェラルの追跡を有効にします。
- 最大LDAPリフェラル数 — 追跡するLDAPリフェラルの最大数。
- 「パスワード変更を有効にする」 — パスワードの有効期限が切れた場合に、ユーザーがパスワードを変更できるようにします。パスワードは、設定されているセキュリティタイプがTLSまたはSSLの場合にのみ変更できます。
- 「ネストされたグループ抽出を有効にする」 — ネストされたグループ抽出機能を有効にします。
- 「最大ネストレベル」 — グループ抽出が許可されるレベルの数。
- 「グループ名識別子」 — LDAPサーバーでグループを一意に識別する名前。
- 「グループ検索属性」 — LDAPグループ検索属性。グループがどのグループに属するかを判断するために使用されます。

- 「グループ検索サブ属性」 —LDAPグループ検索サブ属性。グループがどのグループに属するかを判断するために使用されます。
- 「グループ検索フィルター」 —デフォルトのLDAPグループ検索文字列と組み合わせて検索値を形成する文字列。

4. 「作成」をクリックし、次に「閉じる」をクリックします。

LDAPユーザーのSSH公開鍵認証のサポート

SDXアプライアンスは、ログオン時にSSH公開鍵認証を介してLDAPユーザーを認証できるようになりました。公開鍵のリストは、LDAPサーバーのユーザーオブジェクトに保存されます。認証中、SSHはLDAPサーバーからSSH公開鍵を抽出します。取得された公開鍵のいずれかがSSHをサポートしている場合、ログオンは成功します。

抽出された公開鍵の属性名は、LDAPサーバーとNetScaler SDXアプライアンスの両方に存在する必要があります。

重要

キーベース認証の場合、`/etc/sshd_config` ファイル内の `Authorizedkeysfile` の値を次の側面で設定することにより、公開鍵の場所を指定する必要があります。

```
AuthorizedKeysFile .ssh/authorized_keys
```

システムユーザー。 任意のシステムユーザーの公開鍵の場所は、`/etc/sshd_config` * ファイル内の `Authorizedkeysfile` の値を設定することで指定できます。

LDAPユーザー。 取得された公開鍵は、`/var/pubkey/<user_name>/tmp_authorized_keys-<pid>` ディレクトリに保存されます。`pid` は、同じユーザーからの同時SSHリクエストを区別するために追加される一意の番号です。この場所は、認証プロセス中に公開鍵を保持するための一時的な場所です。認証が完了すると、公開鍵はシステムから削除されます。

ユーザーとしてログインするには、シェลプロンプトから次のコマンドを実行します。

```
$ ssh -i <private key> <username>@<IPAddress>
```

GUIを使用してLDAPサーバーを構成するには：

1. **System > Authentication > LDAP** に移動します。
2. LDAPページで、タブをクリックします。
3. 利用可能なLDAPサーバーのいずれかをクリックします。

4. **Configure Authentication LDAP Server** ページで、**Authentication** を選択します。



注：

LDAPユーザーの認証に「sshPublicKeys」を使用するには、チェックボックスをオフにします。

FQDN名前解決のためのプライマリDNSの追加

サーバーのIPアドレスの代わりにFQDNを使用してRADIUSまたはLDAPサーバーを定義する場合、サーバー名を解決するためにプライマリDNSを手動で設定します。GUIまたはCLIのいずれかを使用できます。

GUIを使用してプライマリDNSを設定するには、**System > Network Configuration > DNS** に移動します。

CLIを使用してプライマリDNSを設定するには、次の手順に従います。

1. Secure Shell (SSH) コンソールを開きます。
2. 管理者資格情報を使用して NetScaler SDX アプライアンスにログインします。
3. `networkconfig` コマンドを実行します。
4. 適切なメニューを選択し、DNS IPv4 アドレスを更新して、変更を保存します。

`networkconfig` コマンドを再度実行すると、更新された DNS アドレスが表示されます。

TACACSサーバーの追加

TACACS認証を設定するには、認証タイプをTACACSとして指定し、TACACS認証サーバーを設定します。

TACACSサーバーを追加するには

1. **Configuration** タブで、**System** の下にある **Authentication** を展開し、**TACACS** をクリックします。
2. 詳細ペインで、**Add** をクリックします。
3. 「TACACSサーバーの作成」ダイアログボックスで、パラメーターの値を入力または選択します。

- 名前 — TACASサーバーの名前

- IPアドレス — TACACSサーバーのIPアドレス
- ポート — TACACSサーバーが実行されているポート。デフォルト値: 49
- タイムアウト — システムがTACACSサーバーからの応答を待機する最大秒数
- TACACSキー — クライアントとサーバー間で共有されるキー。この情報は、システムがTACACSサーバーと通信するために必要です。
- アカウンティング — Management ServiceがTACACSサーバーで監査情報をログに記録できるようにします。
- グループ属性名 — TACACS+サーバーで設定されたグループ属性の名前。

TACACSサーバーの作成(/en-us/sdx/media/create-tacacs-server-citrix.png)

4. 「作成」をクリックし、次に「閉じる」をクリックします。

Management Serviceからリンクアグリゲーションを設定する

リンクアグリゲーションは、複数のイーサネットリンクを1つの高速リンクに結合します。リンクアグリゲーションを設定すると、NetScaler SDXアプライアンスと他の接続デバイス間の通信チャネルの容量と可用性が向上します。集約されたリンクは「チャネル」とも呼ばれます。

ネットワークインターフェイスがチャネルにバインドされている場合、チャネルパラメータがネットワークインターフェイスパラメータよりも優先されます。(つまり、ネットワークインターフェイスパラメータは無視されます。) ネットワークインターフェイスは1つのチャネルにのみバインドできます。

ネットワークインターフェイスがチャネルにバインドされると、そのVLAN構成は破棄されます。インターフェイスは元々属していたVLANから削除され、デフォルトVLANに追加されます。ただし、チャネルを元のVLANまたは新しいVLANに再度バインドできます。たとえば、ネットワークインターフェイス1/2と1/3をID 2のVLAN (VLAN 2) にバインドし、その後それらをチャネルLA/1にバインドすると、ネットワークインターフェイスはデフォルトVLANに移動しますが、チャネルをVLAN 2にバインドできます。

注:

- インターフェイスは1つのチャネルの一部である必要があります。
- チャネルを設定するには、最低2つのインターフェイスが必要です。
- チャネルの一部であるインターフェイスは、NetScalerインスタンスを追加または変更する際に、ネットワーク設定ビューに表示されません。インターフェイスの代わりに、チャネルが一覧表示されます。

1つのインスタンスに割り当てられた3つのインターフェイスを使用してチャンネルを設定し、2番目のインスタンスがこれらのインターフェイスの一部を使用する場合、Management Serviceは2番目のインスタンスをシャットダウンし、ネットワーク設定を変更して、インスタンスを再起動します。たとえば、Instance1とInstance2という2つのインスタンスがあるとします。これらのインスタンスがプロビジョニングされると、インターフェイス10/1、10/2、および10/3はInstance1に割り当てられ、インターフェイス10/1および10/2はInstance2に割り当てられます。インターフェイス10/1、10/2、および10/3でLAチャンネルが作成された場合、Instance1は再起動されません。ただし、Management ServiceはInstance2をシャットダウンし、インターフェイス10/3をInstance2に割り当ててから、Instance2を再起動します。

LAチャンネルからインターフェイスを削除すると、変更はデータベースに保存され、インスタンスを追加または変更する際に、ネットワーク設定ビューにインターフェイスが表示されます。インターフェイスを削除する前は、インターフェイスが属するチャンネルのみが一覧表示されます。

Management Serviceからのチャンネルの構成

チャンネルは手動で構成することも、Link Aggregation Control Protocol (LACP) を使用することもできます。手動で構成されたチャンネルにLACPを適用することはできません。また、LACPによって作成されたチャンネルを手動で構成することもできません。Management Serviceからチャンネルを構成します。その後、NetScalerインスタンスのプロビジョニングまたは変更時にチャンネルを選択します。

LAチャンネルは、リンク冗長性と帯域幅集約を提供するための論理エンティティです。チャンネルの一部であるインターフェイスには、個別のIPアドレスを割り当てることはできません。

注: NetScaler SDXアプライアンスはリンクアグリゲーションをサポートしますが、リンク冗長性はサポートしません。NetScalerリリース13.1ビルド27.x以降では、NetScaler SDXアプライアンスでホストされているNetScaler VPXインスタンスでのリンク冗長性構成は明示的にサポートされていません。

Management Serviceからチャンネルを構成するには

1. **System > Channels** に移動します。
2. 詳細ペインで、**Add** をクリックします。
3. **Add Channel** ダイアログボックスで、次のパラメータを設定します。
 - **チャンネルID** — 作成するLAチャンネルのID。LA/x表記でLAチャンネルを指定します。xは1からインターフェイス数の半分までの範囲です。LAチャンネルの作成後は変更できません。
 - **タイプ** — チャンネルのタイプ。指定可能な値:

- 静的 — データインターフェイスのみで構成されます。
 - アクティブ-アクティブ — 管理インターフェイス0/xのみで構成されます。
 - アクティブ-パッシブ — 管理インターフェイス0/xのみで構成されます。
 - LACP — データインターフェイスと管理インターフェイス0/xで構成されます。
- スループット (静的チャンネルとLACPにのみ適用) — LAチャンネルのスループットの低しい値 (Mbps)。HA構成では、LAチャンネルでHA MONが有効になっており、スループットが指定されたしきい値を下回ると、フェールオーバーがトリガーされます。
 - 帯域幅高 (静的チャンネルおよびLACPにのみ適用)—LAチャンネルの帯域幅使用量に対する高しい値 (Mbps単位)。LAチャンネルの帯域幅使用量が指定された高しい値以上になると、アプライアンスはSNMPトラップメッセージを生成します。
 - 帯域幅標準 (静的チャンネルおよびLACPにのみ適用)—LAチャンネルの帯域幅使用量に対する標準しきい値 (Mbps単位)。LAチャンネルの帯域幅使用量が高しい値を超えた後、指定された標準しきい値以下になると、NetScaler SDXアプライアンスは帯域幅使用量が正常に戻ったことを示すSNMPトラップメッセージを生成します。
4. 「インターフェイス」 タブで、このチャンネルに含めるインターフェイスを追加します。
 5. 「設定」 タブで、次のパラメータを設定します。
 - チャンネル状態 (静的チャンネルにのみ適用)—LAチャンネルを有効または無効にします。
 - LACP時間 (LACPにのみ適用)—LACPDUを受信しない場合、リンクが集約されなくなるまでの時間。この値は、SDXアプライアンスおよびパートナーノード上のリンクアグリゲーションに参加するすべてのポートで一致している必要があります。
 - HA監視—高可用性 (HA) 構成では、チャンネルの障害イベントを監視します。HA MONが有効になっているLAチャンネルの障害は、HAフェイルオーバーをトリガーします。
 - すべてのタグ付け—このチャンネルで送信されるすべてのパケットに4バイトの802.1qタグを追加します。ON設定は、このチャンネルにバインドされているすべてのVLANにタグを適用します。OFF設定は、ネイティブVLAN以外のすべてのVLANにタグを適用します。
 - エイリアス名—LAチャンネルのエイリアス名。読みやすさを向上させるためにのみ使用されます。何らかの操作を実行するには、LAチャンネルIDを指定する必要があります。
 6. 「作成」 をクリックし、「閉じる」 をクリックします。

注

- 0/1および0/2インターフェイスの両方がVPXインスタンスの一部であり、そのインスタンスがクラスターの一部である場合、管理LAを作成することはできません。
- 管理LAがVPXインスタンスの一部であり、そのインスタンスがクラスターの一部である場合、管理LAを削除することはできません。

アクセス制御リスト

アクセス制御リスト (ACL) は、IP トラフィックをフィルタリングし、不正アクセスからアプライアンスを保護するために、ネットワークアプライアンスに適用できる一連の条件です。

NetScaler SDX Management Service GUI で ACL を構成して、アプライアンスへのアクセスを制限および制御できます。

注:

SDX アプライアンスの ACL は、リリース 12.0 57.19 以降でサポートされています。

このトピックには、次のセクションが含まれています。

- 使用ガイドライン
- ACL の構成方法
- ACL ルールに対するその他のアクション
- トラブルシューティング

使用ガイドライン

アプライアンスで ACL を作成する際は、次の点に注意してください。

- SDX アプライアンスをリリース 11.0 57.19 にアップグレードすると、ACL 機能はデフォルトで無効になります。
- SDX 管理者は、SDX アプライアンス上の ACL を介してインバウンドパケットのみを制御できます。
- NetScaler® Application Delivery Management を使用して SDX アプライアンスを管理する場合は、MAS と SDX Management Service 間の通信を許可するために、適切な ACL ルールを作成する必要があります。

- SDXアプライアンス上のVPXのプロビジョニングまたは削除、外部サーバーの追加/削除、SNMP管理などのその他の構成では、既存のACL構成を変更する必要はありません。これらのエンティティとの通信は、管理サービスによって処理されます。

ACLを構成する方法

ACLの構成には、次の手順が含まれます。

- ACL機能を有効にする
- ACLルールを作成する
- ACLルールを有効にする

注:

ACL機能を有効にせずにACLルールを作成できます。ただし、機能が有効になっていない場合、作成後にACLルールを有効にすることはできません。

ACL機能を有効にする

1. ACL機能を有効にするには、SDX管理サービスGUIにログインし、**Configuration > System > ACL**に移動します。
2. トグルボタンを使用して、ACL機能をオンにします。

ACLルール(/en-us/sdx/media/sdx-acl-1-citrix.png)

ACLルールを作成する

1. ACLページで、**Create Rule**をクリックします。
2. **Create Rule**ウィンドウが開きます。次の表に記載されている詳細を追加します。

プロパティ	説明
名前	名前を追加します。
プロトコル	メニューからプロトコルを選択します。デフォルトでは、TCPが選択されています。すべてのプロトコルを許可するには、 ANY を選択できます。
送信元IPアドレス/サブネット	ルールが適用される送信元IPアドレスまたは送信元サブネットを指定します。すべての受信トラフィックにルールを適用する必要がある場合は、 ANY を選択します。
宛先IP	SDX管理サービスのIPアドレスは、宛先IPとして自動入力されます。このフィールドは編集できません。
宛先ポート	ルールが適用される宛先ポートを指定します。すべての宛先ポートにルールを適用する場合は、 ANY を選択します。
アクション	ルールのアクション（許可または拒否）を選択します。
優先度	ルールが評価される順序を指定するために優先度を割り当てます。優先度番号は、ACLルールが受信パケットと照合される順序を決定します。優先度番号が小さいほど、優先度が高くなります。例えば、優

先度番号1は優先度番号1よりも優先度が高くなります。いずれのルールも受信パケットと一致しない場合、パケットはブロックされます。|

3. ルールを作成するには、**OK**をクリックします。

図: ACLルールの例

SDX ACLルール(/en-us/sdx/media/example-sdx-acl-rule-citrix.png)

ルールが作成されると、無効状態になります。ルールを有効にするには、ルールを有効にする必要があります。

注:

ルールを有効にするには、ACL機能が有効になっている必要があります。機能が無効になっている状態でACLルールを有効にしようとすると、「ACL is not running」というメッセージが表示されます。

ACLルールを有効にする

1. 有効にしたいルールにマウスカーソルを合わせ、3つの点がある円をクリックします。
2. メニューから**有効にする**を選択します。
3. または、そのルールのラジオボタンを選択し、**有効にする**タブをクリックします。
4. プロンプトで、**はい**をクリックして確認します。

ACLルールのその他のアクション

ACLルールには、次のアクションを適用できます。

1. ACLルールを無効にする
2. ACLルールを編集する
3. ACLルールを削除する
4. ACLルールの優先順位を振り直す

ACLルールを無効にする

1. 無効にしたいルールにマウスを重ね、3つの点がある円を選択します。
2. リストから**無効にする**をクリックします。
3. または、そのルールのラジオボタンを選択し、**無効にする**タブをクリックします。
4. 確認のため、**はい**をクリックします。

注:

ルールを無効にすると、そのルールは受信トラフィックに適用されなくなります。ただし、ルールの設定はACL設定の下に残ります。

ACLルールを編集する

1. 編集したいルールにマウスを重ね、3つの点がある円を選択します。
2. リストから**ルール**の編集をクリックします。**ルールの変更**ウィンドウが開きます。
3. または、そのルールのラジオボタンを選択し、**ルール**の編集タブをクリックします。**ルールの変更**ウィンドウが開きます。
4. 編集を行い、**OK**をクリックします。

注記:

ルールは、有効状態でも無効状態でも編集できます。すでに有効になっているルールを編集した場合、変更はすぐに適用されます。無効状態のルールの場合、変更はルールを有効にしたときに適用されます。

ACLルールを削除する

1. ルールが無効状態であることを確認してください。
2. 削除したいルールにマウスカーソルを合わせ、3つの点がある円を選択します。リストから**Delete Rule**をクリックします。
3. または、そのルールのラジオボタンを選択し、**Delete Rule**タブをクリックします。
4. 確認のため、**Yes**をクリックします。

注記:

有効状態のルールは削除できません。

ACLルールの優先順位を振り直す

1. 優先順位を振り直したいルールにマウスカーソルを合わせ、3つの点がある円を選択します。リストから****Renumber Priority(s)****をクリックします。
2. または、そのルールのラジオボタンを選択し、**Select Action**タブをクリックします。
3. ****Renumber Priority(s)****を選択します。

4. SDX Management Serviceは、既存のすべてのルールに、10の倍数である新しい優先順位番号を自動的に割り当てます。
5. 要件に応じて優先順位番号を割り当てるためにルールを編集します。ルールの編集方法の詳細については、「ACLルールを編集するには」セクションを参照してください。

図。既存の優先度番号の例



図。優先度が再番号付けされた後、10の倍数で表示される優先度番号の例



トラブルシューティング

ACLルールが不適切に設定されている場合、すべてのユーザーアカウントがアクセスを拒否される可能性があります。不適切なACL設定により、誤ってSDX Management Serviceへのすべてのネットワークアクセスを失った場合は、以下の手順に従ってアクセスを回復してください。

1. SSHと「root」アカウントを使用して、Citrix Hypervisor™管理IPアドレスにログオンします。
2. 管理者権限を使用して、Management Service VMのコンソールにログオンします。
3. コマンド `pfctl -d` を実行します。
4. GUIを介してManagement Serviceにログオンし、それに応じてACLを再構成します。

NetScalerインスタンスのクラスターをセットアップする

1つ以上のSDXアプライアンスにNetScalerインスタンスをプロビジョニングした後、NetScalerインスタンスのクラスターを作成できます。

Citrix®は、Management Serviceからクラスター構成を実行することを推奨しています。VPXインスタンスからクラスター構成を実行すると、Management Serviceは30分ごとの自動検出中に構成を学習します。最悪の場合、クラスタリング情報は30分間検出されません。クラスターは正常に機能する可能性があります。クラスターの依存関係に関するいくつかの重要な検証チェックが見落とされます。Management Serviceは、ADCインスタンスでクラスターを構成する前にこれらのチェックを実行します。したがって、すべてのクラスター構成はManagement Serviceから実行する必要があります。

注:

- クラスターをセットアップするには、NetScalerクラスタリングを理解する必要があります。詳細については、[クラスタリング](#)を参照してください。

- SDXアプライアンス全体にNetScalerインスタンスを持つクラスターの場合、Citrixは3つのSDXアプライアンスからNetScalerインスタンスを使用することを推奨しています。このプロセスにより、最小($n/2 + 1$)ノードというクラスター基準が常に満たされることが保証されます。

図1. SDX NetScalerインスタンスのクラスター



上の図は、同じサブネット上にある3つのSDXアプライアンス、SDX1、SDX2、SDX3を示しています。これらのアプライアンス上のNetScalerインスタンスは、Cluster1とCluster2の2つのクラスターを形成するために使用されます。

- Cluster1には、SDX1上に2つのインスタンスが含まれています。
- Cluster2には、SDX1上に1つのインスタンス、SDX2上に2つのインスタンス、SDX3上にさらに2つのインスタンスが含まれています。

留意事項

- クラスターの各ノードには6 GBのRAMを使用することをお勧めします。
- NetScaler SDX™ アプライアンスでホストされているNetScaler VPXインスタンスには、専用のコアをプロビジョニングする必要があります。
- Mellanoxインターフェイス（50Gおよび100G）を使用したCLAGの形成は、SDXプラットフォームではサポートされていません。
- クラスターのすべてのノードは同じタイプである必要があります。以下の組み合わせでクラスターを形成することはできません。
 - ハードウェアアプライアンスと仮想アプライアンス。
 - NetScaler VPXインスタンスとNetScaler SDXインスタンス。
 - 異なるSDXハードウェアプラットフォーム上のADCインスタンス。
- NetScalerインスタンスはすべて同じバージョンである必要があります、バージョン10.1以降である必要があります。
- NetScalerインスタンスはすべて同じ機能ライセンスを持っている必要があります。
- クラスターに追加された後、個々のNetScalerインスタンスで構成を更新することはできません。すべての変更はクラスターIPアドレスを介して実行する必要があります。
- NetScalerインスタンスはすべて同じリソース（メモリ、CPU、インターフェイスなど）を持っている必要があります。

- バックプレーンMTUは、データインターフェイスMTUより78バイト大きくする必要があります。
- データインターフェイスMTUが9138バイト以内であることを確認してください。
- リリース13.0ビルド82.x以降、クラスターにノードを追加する際にSNIPアドレスを追加するよう求められます。ノードの追加中にSNIPアドレスを動的に作成することもできます。この機能は、厳密な送信元IPアドレスチェックに関するセキュリティ問題に対処するのに役立ちます。
- **重要！** クラスターの削除オプションは注意して使用してください。クラスターの削除をクリックすると、警告なしにクラスターが削除されます。

SDXアプライアンスでクラスターをセットアップする

1. SDXアプライアンスにログインします。
2. **構成**タブで、**NetScaler > クラスター > クラスターインスタンス**に移動します。
3. クラスターを作成する:
 - a. **クラスターの作成**をクリックします。
 - b. 「**クラスターの作成**」ダイアログボックスで、クラスターに必要なパラメーターを設定します。パラメーターの説明については、対応するフィールドにマウスポインターを合わせます。
 - c. 構成の概要を表示するには、「**次へ**」をクリックします。
 - d. クラスターを作成するには、「**完了**」をクリックします。注: L2 VLANが構成されたNetScalerインスタンスがクラスターに追加されると、`add VLAN`コマンドは、`sdxvlan`パラメーターがYesに設定された状態で保存されます。このパラメーターは内部引数であり、SDXクラスター形成中の接続損失を回避するために使用されます。
4. クラスターにノードを追加する:
 - a. **ノードの追加**をクリックします。
 - b. 「**ノードの追加**」ダイアログボックスで、クラスターノードの追加に必要なパラメーターを設定します。パラメーターの説明については、対応するフィールドにマウスポインターを合わせます。
 - c. 構成の概要を表示するには、「**次へ**」をクリックします。
 - d. ノードをクラスターに追加するには、「**完了**」をクリックします。
 - e. 別のノードをクラスターに追加するには、手順1から4を繰り返します。

クラスターを作成したら、クラスターIPアドレスを介してアクセスして構成する必要があります。

クラスターインスタンス内のノードが同じCitrix NetScaler SDXアプライアンスに属している場合、NetScaler SDXアプライアンスが故障すると、クォーラムを失う可能性があります。

クラスターノードは、次の方法を使用して展開できます。

1. 各NetScaler SDXアプライアンスから1つのVPXインスタンスを使用して、複数のクラスターインスタンスを作成します。

例:

SDX1	SDX2	INSTANCEID
VPX1	VPX1	1
VPX2	VPX2	2

1. NetScaler SDXアプライアンスが2台を超える場合は、`quorumType Majority` を使用して、すべてのアプライアンスのVPXインスタンスで単一のクラスターインスタンスを作成します。この場合、VPXインスタンスがすべてのNetScaler SDXアプライアンスに均等に分散されていることを確認してください。

例1:

SDX1	SDX2	SDX3	インスタンスID
VPX1	VPX1	VPX1	1
VPX2	VPX2	VPX2	NA
VPX3	VPX3	VPX3	NA

例2:

SDX1	SDX2	SDX3	インスタンスID
VPX1	VPX1	VPX1	1
VPX2	VPX2	VPX2	N/A
VPX3	VPX3	VPX3	N/A
VPX4	NA	NA	NA

- すべてのNetScaler SDXデバイスからすべてのVPXインスタンスを使用して、単一のクラスターインスタンスを作成します。ただし、`quorum type NONE` を使用します。これにはいくつかの制限があります。

例:

SDX1	SDX2	INSTANCEID
VPX1	VPX1	1
VPX2	VPX2	2
VPX3	NA	NA

`-quorumType` パラメーターが `NONE` に設定されている場合の制限事項:

- 単一障害点によるネットワークパーティションを回避するため、トポロジはクラスターノード間に冗長リンクを持つ必要があります。
- ノードの追加や削除などのクラスター操作中に、クラスターが不安定になる可能性があります。

注:

SDXアプライアンスのNetScalerインスタンスを少なくとも1つ持つNetScalerクラスターの更新されたリストを取得するには、**Rediscover**オプションを使用します。

あるSDXアプライアンスに存在するNetScalerインスタンスを、別のSDXアプライアンスで構成されたクラスターに追加する

- NetScalerインスタンスを追加したいSDXアプライアンスにログオンします。
- Configuration**タブで、**NetScaler**に移動し、**Clusters**をクリックします。
- Add Node**をクリックします。
- Add Node**ダイアログボックスで、クラスターノードの追加に必要なパラメーターを設定します。パラメーターの説明については、対応するフィールドにマウスポインターを合わせます。
注：クラスターIPアドレスとクラスターIPパスワードのパラメーター値が、ノードを追加したいクラスターのものであることを確認してください。
- 構成の概要を表示するには、**Next**をクリックします。
- ノードをクラスターに追加するには、**Finish**をクリックします。

クラスタリンクアグリゲーションの構成

クラスタリンクアグリゲーションは、その名の通り、クラスタノードインターフェースのグループをチャンネルに結合します。これはNetScalerリンクアグリゲーション (LA) の拡張機能です。唯一の違いは、リンクアグリゲーションではインターフェースが同じデバイス上にある必要があるのに対し、クラスタリンクアグリゲーションではインターフェースがクラスタの異なるノード上にある点です。リンクアグリゲーションの詳細については、「リンクアグリゲーションの構成」([/ja-jp/citrix-adc/current-release/networking/interfaces/configuring-link-aggregation.html](https://ja-jp.citrix-adc/current-release/networking/interfaces/configuring-link-aggregation.html))を参照してください。

たとえば、2つのSDXアプライアンスにまたがる6ノードクラスタで、すべての6ノードがアップストリームスイッチに接続されている場合を考えます。インターフェース0/1/2、1/1/3、2/1/4、3/1/2、4/1/3、および5/1/4をバインドすることで、クラスタLAチャンネル (CLA/1) が形成されます。



クラスタLAチャンネルには、次の属性があります。

- 各チャンネルは、クラスタノード間で合意された一意のMACアドレスを持ちます。
- このチャンネルは、ローカルおよびリモートのSDXノードのインターフェースの両方をバインドできます。
- クラスタでは、最大4つのクラスタLAチャンネルがサポートされます。
- 各クラスタLAチャンネルには、最大16個のインターフェースをバインドできます。
- バックプレーンインターフェースはクラスタLAチャンネルの一部にすることはできません。
- インターフェースがクラスタLAチャンネルにバインドされている場合、チャンネルパラメータがネットワークインターフェースパラメータよりも優先されます。
- ネットワークインターフェースは1つのチャンネルにのみバインドできます。
- クラスタLAチャンネル (例: CLA/1) またはそのメンバーインターフェースで、クラスタノードへの管理アクセスを構成しないでください。ノードがINACTIVEの場合、対応するクラスタLAインターフェースはPOWER OFFとマークされ、管理アクセスが失われます。



クラスタIPアドレスと外部接続デバイスで同様の構成を実装します。可能であれば、MACアドレスではなくIPアドレスまたはポートに基づいてトラフィックを分散するようにアップストリームスイッチを構成してください。

留意点:

- LACP を有効にします (LACP モードを ACTIVE または PASSIVE のいずれかに指定します)。
注: NetScaler クラスターと外部接続デバイスの両方で LACP モードが PASSIVE に設定されていないことを確認してください。
- クラスター LA チャネルを作成する場合、LACP キーの値は 5 から 8 の範囲で指定できます。これらの LACP キーは、CLA/1、CLA/2、CLA/3、CLA/4 にマッピングされます。
- SDX アプライアンスでは、クラスターリンクアグリゲーショングループ (CLAG) のメンバーインターフェイスを他の仮想マシンと共有することはできません。
- アップストリームスイッチで、クラスターノードでの長時間のトラフィックブラックホールを回避するために、LACP タイムアウトを「short」に設定します。この設定は、LACP タイムアウトが経過するまで、CLAG とそのメンバーインターフェイスの電源オフがアップストリームスイッチに通知されない場合に役立ちます。

前提条件:

NetScaler インスタンスのクラスターを作成します。クラスターのノードは、同じ SDX アプライアンス上にある NetScaler インスタンス、または同じサブネットを利用可能な他の SDX アプライアンス上にある NetScaler インスタンスのいずれかです。

Management Service を使用してクラスター LA チャネルを構成するには:

1. SDX アプライアンスにログオンします。
2. **Configuration** タブで、**Citrix® ADC** に移動し、**Clusters** をクリックします。
3. **Cluster Instances** ページで、クラスターを選択し、**CLAG** をクリックします。



4. **Create CLAG** ダイアログボックスで、次の操作を行います。
 - a. **Channel ID** ドロップダウンリストで、クラスター LA チャネル ID を選択します。
 - b. **Interfaces** セクションの **Available** 選択ボックスからインターフェイスを選択し、**+** をクリックします。
 - c. 選択されたインターフェイスは、**設定済み** 選択ボックスの下に表示されます。
5. **設定** セクションで、以下を実行します。
 - a. **エイリアス** フィールドに、クラスター LA チャネルの代替名を入力します。
 - b. **LACP タイムアウト** フィールドで、リンクが LACPDU を受信しない場合に、リンクが集約されない間隔を定義するために、以下のいずれかの値を選択します。

この値は、SDXアプライアンスおよびパートナーノード上のリンクアグリゲーションに参加するすべてのポートで一致している必要があります。

- 長 – 30秒
- 短 – 1秒

- c. 高可用性 (HA) 構成の場合、チャンネルの障害イベントを監視するために、**HA監視チェック**ボックスを選択します。HA MONが有効になっているLAチャンネルの障害は、HAフェイルオーバーをトリガーします。
- d. **すべてタグ付け**を選択して、このチャンネルで送信されるすべてのパケットに4バイトの802.1qタグを追加します。**ON**設定は、このチャンネルにバインドされているすべてのVLANにタグを適用します。OFFは、ネイティブVLAN以外のすべてのVLANにタグを適用します。

6. **作成**をクリックして、いずれかのSDXアプライアンスのCLAGを構成します。

CLAGを作成する(/en-us/sdx/media/add-clag1-citrix.png)

7. **確認**ダイアログボックスで、**はい**をクリックして、他のSDXアプライアンスのCLAG設定を更新します。

注:

- **いいえ**を選択した場合、CLAGは構成されません。
- 他のSDXアプライアンスのCLAG設定を手動で更新します。
- MTU設定は両方のSDXアプライアンスで同じである必要があります。MTU設定はいずれかのSDXアプライアンスで手動で変更する必要があります。

8. **CLAGs**ダイアログボックスでMTU設定を変更するには、次の手順を実行します。
 - a. **CLA/1**を選択し、**編集**をクリックします。
 - b. **CLAGの構成**ダイアログボックスで、**MTU**フィールドにMTUを手動で設定し、**OK**をクリックします。
9. **確認**ダイアログボックスで、**はい**をクリックします。

管理サービスに安全にアクセスするためのSSL暗号の構成

NetScaler SDXアプライアンスでサポートされているSSL暗号のリストからSSL暗号スイートを選択できます。SSL暗号の任意の組み合わせをバインドして、HTTPS経由でSDX管理サービスに安全にアクセスできます。SDXアプライアンスは、類似の暗号の組み合わせである37の事前定義された暗号グループを提供し、サポートされているSSL暗号のリストからカスタム暗号グループを作成できます。

制限事項

- 鍵交換が「DH」または「ECC-DHE」の暗号のバインドはサポートされていません。
- 認証が「DSS」の暗号のバインドはサポートされていません。
- サポートされているSSL暗号リストに含まれていない暗号のバインド、またはこれらの暗号をカスタム暗号グループに含めることはサポートされていません。

サポートされているSSL暗号

次の表に、サポートされているSSL暗号を示します。「プロトコル」列の値は、サポートされている最も低いプロトコルです。たとえば、SSLv3がリストされている場合、SSLv3/TLSv1/TLSv1.1/TLSv1.2はすべてサポートされます。

CITRIX暗号名	OPENSSL暗号名	16進コード	プロトコル	鍵交換アルゴリズム	認証アルゴリズム	メッセージ認証コード (MAC) アルゴリズム
TLS1-AES-256-CBC-SHA	AES256-SHA	0x0035	エスエスエルブイスリー	RSA	RSA	AES(256)
TLS1-AES-128-CBC-SHA	AES128-SHA	0x002F	エスエスエルブイスリー	RSA	RSA	AES(128)
TLS1.2-AES-256-SHA256	AES256-SHA256	0x003D	TLSv1.2	RSA	RSA	AES(256)
TLS1.2-AES-128-SHA256	AES128-SHA256	0x003C	TLSv1.2	RSA	RSA	AES(128)

CITRIX暗号名	OPENSSL暗号名	16進コード	プロトコル	鍵交換アルゴリズム	認証アルゴリズム	メッセージ認証コード (MAC) アルゴリズム
TLS1.2-AES256-GCM-SHA384	AES256-GCM-SHA384	0x009D	TLSv1.2	RSA	RSA	AES-GCM(256)
TLS1.2-AES128-GCM-SHA256	AES128-GCM-SHA256	0x009C	TLSv1.2	RSA	RSA	AES-GCM(128)
TLS1-ECDHE-RSA-AES256-SHA	ECDHE-RSA-AES256-SHA	0xC014	SSLバージョン3	ECC-DHE	RSA	AES(256)
TLS1-ECDHE-RSA-AES128-SHA	ECDHE-RSA-AES128-SHA	0xC013	SSLバージョン3	ECC-DHE	RSA	AES(128)
TLS1.2-ECDHE-RSA-AES-256-SHA384	ECDHE-RSA-AES256-SHA384	0xC028	TLSv1.2	ECC-DHE	RSA	AES(256)
TLS1.2-ECDHE-RSA-AES-128-SHA256	ECDHE-RSA-AES128-SHA256	0xC027	TLSv1.2	ECC-DHE	RSA	AES(128)
TLS1.2-ECDHE-RSA-AES256-	ECDHE-RSA-AES256-	0xC030	TLSv1.2	ECC-DHE	RSA	AES-GCM(256)

CITRIX暗号名	OPENSSL暗号名	16進コード	プロトコル	鍵交換アルゴリズム	認証アルゴリズム	メッセージ認証コード (MAC) アルゴリズム
GCM-SHA384	GCM-SHA384					
TLS1.2-ECDHE-RSA-AES128-GCM-SHA256	ECDHE-RSA-AES128-GCM-SHA256	0xC02F	TLSv1.2	ECC-DHE	RSA	AES-GCM(128)
TLS1.2-DHE-RSA-AES-256-SHA256	DHE-RSA-AES256-SHA256	0x006B	TLSv1.2	DH	RSA	AES(256)
TLS1.2-DHE-RSA-AES-128-SHA256	DHE-RSA-AES128-SHA256	0x0067	TLSv1.2	DH	RSA	AES(128)
TLS1.2-DHE-RSA-AES256-GCM-SHA384	DHE-RSA-AES256-GCM-SHA384	0x009F	TLSv1.2	DH	RSA	AES-GCM(256)
TLS1.2-DHE-RSA-AES128-GCM-SHA256	DHE-RSA-AES128-GCM-SHA256	0x009E	TLSv1.2	DH	RSA	AES-GCM(128)
TLS1-DHE-RSA-	DHE-RSA-	0x0039	SSLバージョン3	DH	RSA	AES(256)

CITRIX暗 号名	OPENSSL暗号名	16進コード	プロトコル	鍵交換アル ゴリズム	認証アルゴ リズム	メッセージ 認証コード (MAC) ア ルゴリズム
AES-256- CBC-SHA	AES256- SHA					
TLS1- DHE- RSA- AES-128- CBC-SHA	DHE- RSA- AES128- SHA	0x0033	エスエス エルv3	DH	RSA	AES(128)
TLS1- DHE- DSS- AES-256- CBC-SHA	DHE- DSS- AES256- SHA	0x0038	エスエス エルv3	DH	DSS	AES(256)
TLS1- DHE- DSS- AES-128- CBC-SHA	DHE- DSS- AES128- SHA	0x0032	エスエス エルブイ スリー	DH	DSS	AES(128)
TLS1- ECDHE- RSA- DES- CBC3- SHA	ECDHE- RSA- DES- CBC3- SHA	0xC012	エスエス エルブイ スリー	ECC- DHE	RSA	3DES(16 8)
SSL3- EDH- RSA- DES- CBC3- SHA	EDH- RSA- DES- CBC3- SHA	0x0016	エスエス エルブイ スリー	DH	RSA	3DES(16 8)
SSL3- EDH- DSS- DES-	EDH- DSS- DES-	0x0013	エスエス エルブイ スリー	DH	DSS	3DES(16 8)

CITRIX暗 号名	OPENSSL暗号名	16進コード	プロトコル	鍵交換アル ゴリズム	認証アルゴ リズム	メッセージ 認証コード (MAC) ア ルゴリズム
CBC3- SHA	CBC3- SHA					
TLS1- ECDHE- RSA- RC4-SHA	ECDHE- RSA- RC4-SHA	0xC011	エスエ エルブイ スリー	ECC- DHE	RSA	RC4(128)
SSL3- DES- CBC3- SHA	DES- CBC3- SHA	0x000A	SSLバー ジョン3	RSA	RSA	3DES(16 8)
SSL3- RC4-SHA	RC4-SHA	0x0005	SSLバー ジョン3	RSA	RSA	RC4(128)
SSL3- RC4-MD5	RC4-MD5	0x0004	エスエ エルブイ スリー	RSA	RSA	RC4(128)
SSL3- DES- CBC-SHA	DES- CBC-SHA	0x0009	エスエ エルブイ スリー	RSA	RSA	DES(56)
SSL3- EXP- RC4-MD5	EXP- RC4-MD5	0x0003	エスエ エルブイ スリー	RSA(512)	RSA	RC4(40)
SSL3- EXP- DES- CBC-SHA	EXP- DES- CBC-SHA	0x0008	エスエ エルブイ スリー	RSA(512)	RSA	DES(40)
SSL3- EXP- RC2- CBC- MD5	EXP- RC2- CBC- MD5	0x0006	エスエ エルブイ スリー	RSA(512)	RSA	RC2(40)

CITRIX暗 号名	OPENSSL暗号名	16進コード	プロトコル	鍵交換アル ゴリズム	認証アルゴ リズム	メッセージ 認証コード (MAC) ア ルゴリズム
SSL2- DES- CBC- MD5	DHE- DSS- AES128- SHA256	0x0040	エスエス エルバイ ツー	RSA	RSA	DES(56)
SSL3- EDH- DSS- DES- CBC-SHA	EDH- DSS- DES- CBC-SHA	0x0012	SSLv3 プ ロトコル	DH	DSS	DES(56)
SSL3- EXP- EDH- DSS- DES- CBC-SHA	EXP- EDH- DSS- DES- CBC-SHA	0x0011	SSLv3 プ ロトコル	DH(512)	DSS	DES(40)
SSL3- EDH- RSA- DES- CBC-SHA	EDH- RSA- DES- CBC-SHA	0x0015	SSLv3	DH	RSA	DES(56)
SSL3- EXP- EDH- RSA- DES- CBC-SHA	EXP- EDH- RSA- DES- CBC-SHA	0x0014	SSLv3	DH(512)	RSA	DES(40)
SSL3- ADH- RC4-MD5	ADH- RC4-MD5	0x0018	SSLバー ジョン3	DH	なし	RC4(128)
SSL3- ADH- DES-	ADH- DES-	0x001B	SSLバー ジョン3	DH	なし	3DES(16 8)

CITRIX暗 号名	OPENSSL暗号名	16進コード	プロトコル	鍵交換アル ゴリズム	認証アルゴ リズム	メッセージ 認証コード (MAC) ア ルゴリズム
CBC3- SHA	CBC3- SHA					
SSL3- ADH- DES- CBC-SHA	ADH- DES- CBC-SHA	0x001A	SSLv3プ ロトコル	DH	なし	DES(56)
TLS1- ADH- AES-128- CBC-SHA	ADH- AES128- SHA	0x0034	エスエス エルバイ スリー	DH	なし	AES(128)
TLS1- ADH- AES-256- CBC-SHA	ADH- AES256- SHA	0x003A	エスエス エルバイ スリー	DH	なし	AES(256)
SSL3- EXP- ADH- RC4-MD5	EXP- ADH- RC4-MD5	0x0017	SSLv3プ ロトコル	DH(512)	なし	RC4(40)
SSL3- EXP- ADH- DES- CBC-SHA	EXP- ADH- DES- CBC-SHA	0x0019	SSLバー ジョン3	DH(512)	なし	DES(40)
SSL3- NULL- MD5	NULL- MD5	0x0001	エスエス エルバイ スリー	RSA	RSA	なし
SSL3- NULL- SHA	NULL- SHA	0x0002	エスエス エルバイ スリー	RSA	RSA	なし

事前定義された暗号グループ

次の表に、SDXアプライアンスによって提供される事前定義された暗号グループを示します。

暗号グループ名	説明
ALL	SDXアプライアンスでサポートされているすべての暗号（NULL暗号を除く）
DEFAULT	暗号強度が128ビット以上のデフォルトの暗号リスト
kRSA	キー交換アルゴリズムがRSAである暗号
kEDH	キー交換アルゴリズムがEphemeral-DHである暗号
DH	キー交換アルゴリズムがDHである暗号
EDH	鍵交換/認証アルゴリズムがDHの暗号
aRSA	認証アルゴリズムがRSAの暗号
aDSS	認証アルゴリズムがDSSの暗号
aNULL	認証アルゴリズムがNULLの暗号
DSS	認証アルゴリズムがDSSの暗号
DES	暗号化アルゴリズムがDESの暗号
3DES	暗号化アルゴリズムが3DESの暗号
RC4	暗号化アルゴリズムがRC4の暗号
RC2	Enc algo が RC2 の暗号
NULL	Enc algo が NULL の暗号
MD5	MAC algo が MD5 の暗号
SHA1	MAC algo が SHA-1 の暗号
SHA	MAC algo が SHA の暗号

暗号グループ名	説明
NULL	Enc algo が NULL の暗号
RSA	Key-ex/Auth algo が RSA の暗号
ADH	鍵交換アルゴリズムがDHで、認証アルゴリズムがNULLの暗号スイート
エスエスエルバイツー	SSLv2プロトコルの暗号スイート

ティーエルエスバイワン	SSLv3/TLSv1プロトコルの暗号スイート
TLSv1_ONLY	TLSv1プロトコルの暗号スイート
EXP	エクスポート暗号スイート
EXPORT	エクスポート暗号スイート
EXPORT40	40ビット暗号化のエクスポート暗号スイート
EXPORT56	56ビット暗号化のエクスポート暗号
LOW	低強度の暗号 (56ビット暗号化)
MEDIUM	中強度の暗号 (128ビット暗号化)
HIGH	高強度の暗号 (168ビット暗号化)
AES	AES暗号
FIPS	FIPS承認暗号
ECDHE	楕円曲線一時DH暗号
AES-GCM	暗号化アルゴリズムがAES-GCMの暗号
SHA2	MACアルゴリズムがSHA-2の暗号

事前定義された暗号グループを表示する

事前定義された暗号グループを表示するには、**構成**タブのナビゲーションペインで**管理サービス**を展開し、**暗号グループ**をクリックします。

カスタム暗号グループを作成する

サポートされているSSL暗号のリストから、カスタム暗号グループを作成できます。

カスタム暗号グループを作成するには：

1. **構成**タブのナビゲーションペインで**管理サービス**を展開し、**暗号グループ**をクリックします。
2. **暗号グループ**ペインで、**追加**をクリックします。
3. **暗号グループの作成**ダイアログボックスで、次の操作を実行します。
 - a. **グループ名**フィールドに、カスタム暗号グループの名前を入力します。
 - b. **暗号グループの説明**フィールドに、カスタム暗号グループの簡単な説明を入力します。
 - c. **暗号スイート**セクションで、**追加**をクリックし、サポートされているSSL暗号のリストに含める暗号を選択します。
 - d. **作成**をクリックします。

既存のSSL暗号バインディングを表示する

既存の暗号バインディングを表示するには、**Configuration**タブのナビゲーションペインで、**System**を展開し、**System Settings**の下にある**Configure SSL Settings**をクリックします。

SSL設定の構成(/en-us/sdx/media/configure-ssl-settings-citrix.png)

注:

Management Serviceの最新バージョンにアップグレードした後、既存の暗号スイートのリストにはOpenSSL名が表示されます。アップグレードされたManagement Serviceから暗号をバインドすると、表示はCitrix®の命名規則を使用します。

HTTPSサービスに暗号をバインドする

1. **Configuration**タブのナビゲーションペインで、**System**をクリックします。
2. **System**ペインのSystem Settingsの下で、**Configure SSL Settings**をクリックします。
3. **Edit Settings**ペインで、**Ciphers Suites**をクリックします。
4. **Ciphers Suites**ペインで、次のいずれかを実行します。
 - 定義済みの暗号グループから暗号グループを選択するには、**Cipher Groups**を選択し、**Cipher Groups**リストから暗号グループを選択して、**OK**をクリックします。

- サポートされている暗号のリストから選択するには、**Cipher Suites**チェックボックスをオンにし、**Add**をクリックして暗号を選択し、**OK**をクリックします。

SDXアプライアンスの構成データをバックアップおよび復元する

NetScaler SDXアプライアンスのバックアッププロセスは、以下の内容を含むバックアップファイルを作成する単一ステップのプロセスです。

- シングルバンドルイメージ:
 - Citrix Hypervisor™ イメージ
 - Citrix Hypervisor のホットフィックスと補足パック
 - Management Service イメージ
- XVA イメージ
- アップグレードイメージ
- SDX構成
- 構成

バックアップフォルダは /var/mps/backup/ です。

現在の構成をバックアップする

1. **構成**タブのナビゲーションペインで、**Management Service**を展開し、バックアップファイルをクリックします。
2. バックアップファイルペインで、バックアップをクリックします。
3. 新しいバックアップファイルダイアログボックスで、バックアップファイルを暗号化するには、ファイルをパスワードで保護チェックボックスをオンにします。
4. 「**Password**」フィールドと「**Confirm Password**」フィールドに、バックアップファイルのパスワードを入力して確認します。
5. 「**Continue**」をクリックします。

バックアッププロセスにより、バックアップファイルが作成されます。バックアップファイルのファイル名には、Management Service の現在の IP アドレスと、バックアップが取得されたときのタイムスタンプが含まれます。バックアップファイルに不整合がないか確認するには、SDX GUI から「**Configuration > System > Events/Alarms**」に移動します。

スケジュールされたバックアップ

デフォルトでは、SDX はバックアップポリシーを使用して24時間ごとにバックアップを作成します。バックアップポリシーを使用すると、SDX アプライアンスに保持するバックアップファイルの数を定義できます。また、スケジュールされたバックアップファイルをパスワードで暗号化して、バックアップファイルのセキュリティを確保することもできます。

バックアップポリシーの編集

1. 「**Configuration**」 タブで、「**System**」 をクリックします。
2. 「**Policy Administration**」 ペインで、「**Backup Policy**」 をクリックします。
3. 「**Configure backup policy**」 ペインで、次の操作を実行します。
 - a. 「**Previous backups to retain**」 フィールドに、保持するバックアップファイルの数を入力します。
 - b. バックアップファイルを暗号化するには、「**Encrypt Backup File**」 チェックボックスをオンにします。
 - c. 「**Password**」 フィールドと 「**Confirm Password**」 フィールドに、バックアップファイルを暗号化するためのパスワードを入力して確認します。

バックアップファイルを外部バックアップサーバーに手動で転送する

バックアップファイルを手動で転送する前に、外部バックアップサーバーの詳細があることを確認してください。

バックアップファイルを外部バックアップサーバーに転送する

1. 「**Configuration**」 タブのナビゲーションペインで、「**Management Service**」 を展開し、「**Backup Files**」 をクリックします。
2. 「**Backup Files**」 ペインで、バックアップファイルを選択し、「**Transfer**」 をクリックします。
3. 「**Server**」 フィールドに、外部バックアップサーバーのホスト名またはIPアドレスを入力します。
4. 「**User Name**」 フィールドと 「**Password**」 フィールドに、外部バックアップサーバーにアクセスするためのユーザー名とパスワードを入力します。
5. 「**Port**」 フィールドに、ポート番号を入力します。
6. 「**Transfer Protocol**」 フィールドで、バックアップファイルを外部バックアップサーバーに転送するために使用するプロトコルを選択します。

7. 「**Directory Path**」フィールドに、バックアップファイルを保存する外部バックアップサーバーのディレクトリパスを入力します。
8. バックアップファイルを外部バックアップサーバーに転送した後、SDXアプライアンスからバックアップファイルを削除するには、「**Delete file from Management Service**」を選択します。
9. 「**OK**」をクリックします。

アプライアンスを復元する

SDXアプライアンスをバックアップファイルで利用可能な構成に復元できます。アプライアンスの復元中、現在のすべての構成は削除されます。

注意事項:

- 別のSDXアプライアンスのバックアップファイルを使用してSDXアプライアンスを復元する前に、バックアップファイルで利用可能な設定に従って管理サービスのネットワーク設定を追加します。
- バックアップが取得されたプラットフォームバリエーションが、復元しようとしているプラットフォームバリエーションと同じであることを確認してください。2つの異なるプラットフォームバリエーション間でバックアップファイルを復元することはサポートされていません。
- Citrix®は、ネットワーク構成が設定された後にはのみSDXバックアップを復元することを推奨します。SVMには次のネットワーク設定を指定できます。
 - SVM IPアドレス
 - ハイパーバイザーIPアドレス
 - サブネットマスク
 - ゲートウェイ
 - DNSサーバー

バックアップファイルからアプライアンスを復元する

1. **Configuration**タブのナビゲーションペインで、**Management Service**を展開し、**Backup Files**をクリックします。
2. **Backup Files**ペインで、バックアップファイルをクリックし、**OK**をクリックします。
3. **Restore**ダイアログボックスで、**Appliance Restore**を選択し、**Proceed**をクリックします。

アプリケーション復元のさまざまなコンポーネントが表示されます。

- ライセンス

- SDXイメージ
- XVAファイル
- NetScaler構成
- 概要

バックアップファイルに必要なコンポーネントが不足している場合、続行する前に不足している要素をアップロードするよう求められます。

現在のSDXシングルバンドルイメージバージョンでバックアップファイルを復元できるかどうかについては、次の表を参照してください。シングルバンドルイメージの経験則として、以前のバージョンのバックアップは、それ以降のバージョンでは復元できません。

現在のSDXシングルバンドルイメージバージョン	バックアップファイルバージョン
11.1	11.1、12.0、12.1、13.0はサポートされています。11.0はサポートされていません。
12.0	12.0、12.1、13.0はサポートされています。11.0および11.1はサポートされていません。
12.1	12.1、13.0はサポートされています。11.0、11.1、12.0はサポートされていません。
13.0	13.0はサポートされています。11.0、11.1、12.0、12.1はサポートされていません。
13.1	13.1はサポートされています。11.0、11.1、12.0、12.1、13.0はサポートされていません。

4. **License** ページで、有効なライセンスが存在することを確認し、**Next** をクリックします。
5. 「**SDX Image**」 ページが表示されます。SDXイメージがリストアの実行に不要な場合は、「**Next**」 をクリックします。それ以外の場合は、プロンプトが表示されたら有効なSDXイメージをアップロードし、「**Next**」 をクリックします。
6. 「**XVA File**」 ページが開きます。すべてのインスタンスのXVAイメージが存在する場合は、「**Next**」 をクリックします。バックアップファイルにいずれかのインスタンスのXVAファイルがない場合は、アップロードするか、このインスタンスのリストアをスキップできます。「**Next**」 をクリックして次のページに進みます。

7. NetScaler構成ページが開きます。NetScaler構成ファイルは必須ではありません。構成をリストアせずにインスタンスをプロビジョニングできます。バックアップファイルにNetScaler構成ファイルがない場合は、インスタンスのプロビジョニングのみを進めるか、インスタンスのリストアをスキップできます。「**Next**」をクリックして次のページに進みます。
8. サマリーページに、バックアップファイルに存在するすべてのインスタンスに関する以下の詳細が表示されます。
 - IPアドレス
 - ホスト名
 - SDXバージョン
 - XVAバージョン
 - バージョンビット
 - リストア：アプライアンスまたはインスタンスがリストアの準備ができている場合は、チェックマークが表示されます。準備ができていない場合は、バツ印が表示されます。
 - エラーメッセージ：アプライアンスまたはインスタンスがリストアの準備ができていない場合は、その理由を説明するエラーメッセージが表示されます。
9. 「**Restore**」をクリックして、アプリケーションのリストアプロセスを完了します。

NetScalerインスタンスをリストアする

SDXアプライアンスのNetScalerインスタンスを、バックアップファイルで利用可能なNetScalerインスタンスにリストアできます。

注意点：VPXインスタンスは、次の場合にリストアに失敗します。

- インスタンスに管理NICが割り当てられていない場合、および
- インスタンスがLACPを介してのみSDX Management Serviceから管理されている場合。SDX Management Serviceはチャンネル構成を自動的に復元できないため、復元は失敗します。この問題を回避するには、VPXインスタンスの復元を完了するために、チャンネル構成を手動で復元してください。

バックアップファイル内のNetScalerインスタンスを復元するには：

1. 「**Configuration**」タブのナビゲーションペインで、「**Management Service**」を展開し、「**Backup Files**」をクリックします。
2. 「**Backup Files**」ペインで、バックアップファイルを選択し、「**Restore**」をクリックします。

3. 「**Restore**」ダイアログボックスで、「**Instance Restore**」を選択します。
4. 復元するNetScalerインスタンスを選択し、「**Proceed**」をクリックします。
5. (オプション) バックアップファイルが暗号化されている場合は、プロンプトが表示されたらパスワードを入力し、「**OK**」をクリックします。

注：

復元されるインスタンスを実行するSDXアプライアンスに、適切なXVA、ビルドイメージ、およびチャネル構成が存在することを確認してください。

アプライアンスのリセットを実行する

NetScaler SDXアプライアンスでは、次のことができます。

- アプライアンスの構成をリセットします。

注:

構成をリセットするときは、アプライアンスのシリアル番号をパスワードとして使用してログオンする必要があります。

- アプライアンスを工場出荷時のバージョンにリセットします。
- アプライアンスを特定のシングルバンドルイメージバージョンにリセットします。

アプライアンスのリセットを実行する前に、アプライアンスにプロビジョニングされているすべてのNetScalerインスタンスの設定を含む、アプライアンスに保存されているすべてのデータをバックアップしてください。

Citrix®は、ファイルをアプライアンスの外部に保存することをお勧めします。アプライアンスのリセットを実行すると、Management Serviceとの現在のすべてのクライアントセッションが終了します。追加の構成タスクを実行するには、Management Serviceに再度ログオンしてください。データを復元する準備ができたなら、Management Serviceを使用してバックアップファイルをインポートします。

Management Serviceは、アプライアンスをリセットするための次のオプションを提供します。

- 構成のリセット
- ファクトリーリセット

- クリーンインストール

アプライアンスの構成をリセットする

Management Serviceは、アプライアンスの構成をリセットするための「構成のリセット」オプションを提供します。「構成のリセット」オプションは、次の処理を実行します。

- VPXインスタンスを削除します。
- SSL証明書ファイルとキーファイルを削除します。
- ライセンスファイルとテクニカルアーカイブファイルを削除します。
- アプライアンスのNTP設定を削除します。
- タイムゾーンをUTCに復元します。
- プルーニングポリシーとバックアップポリシーをデフォルト設定に復元します。
- Management Serviceイメージを削除します。
- NetScaler SDXイメージを削除します。
- アプライアンスで最後にアクセスされたイメージファイルを除く、すべてのXVAイメージを削除します。
- デフォルトのインターフェイス設定を復元します。
- デフォルトプロファイル、ユーザー、システム設定を含む、アプライアンスのデフォルト設定を復元します。
- Citrix Hypervisor™とManagement Serviceのデフォルトパスワードを復元します。
- Management Serviceを再起動します。

アプライアンスの設定をリセットする

1. **設定 > システム > システム管理グループ** に移動します。
2. 「アプライアンスのリセット」をクリックします。
3. 「アプライアンスのリセット」ダイアログボックスで、「リセットタイプ」リストから「**構成のリセット**」を選択します。
4. 「OK」をクリックします。

アプライアンスを工場出荷時のバージョンにリセットする

マネジメントサービスには、アプライアンスを工場出荷時のバージョンにリセットするためのファクトリリセットオプションが用意されています。ファクトリリセットオプションは、マネジ

メントサービスとCitrix Hypervisorの現在のIPアドレスを、マネジメントサービスとCitrix HypervisorのデフォルトのIPアドレスにリセットします。

アプライアンスに保存されているすべてのデータ（アプライアンスにプロビジョニングされているすべてのNetScalerインスタンスの設定を含む）をバックアップしてください。Citrixは、ファイルをアプライアンスの外部に保存することを推奨します。ファクトリリセットを実行すると、マネジメントサービスとの現在のすべてのクライアントセッションが終了します。追加の構成タスクを実行するには、マネジメントサービスに再度ログオンしてください。データを復元する準備ができたなら、マネジメントサービスを使用してバックアップファイルをインポートします。

重要

ファクトリリセットを実行する前に、シリアルコンソールケーブルがアプライアンスに接続されていることを確認してください。

アプライアンスを工場出荷時のバージョンにリセットする

1. **構成 > システム > システム管理**に移動します。
2. 「アプライアンスのリセット」をクリックします。
3. 「アプライアンスのリセット」ダイアログボックスで、「リセットタイプ」リストから「ファクトリリセット」を選択します。
4. 「OK」をクリックします。

アプライアンスをシングルバンドルイメージバージョンにリセットする

マネジメントサービスには、アプライアンスに任意のバージョンのシングルバンドルイメージをインストールできるクリーンインストールオプションが用意されています。これにより、新しいデフォルトのブートイメージとしてシングルバンドルイメージを新規インストールできます。クリーンインストールでは、SDXアプライアンスの既存の構成（ネットワーク設定を除く）が削除されます。

注記:

SDXアプライアンスがソフトウェアバージョン11.0以前で出荷された場合、バージョン13.1以降へのクリーンインストールは失敗します。

クリーンインストールオプションは以下でサポートされています。

シングルバンドルイメージバージョン	SDXプラットフォーム
11.0.xx	SDX 14xxx、SDX 25xxx。注記: クリーンインストールオプションは、10Gのファクトリパーティションを持つ他のSDXプラットフォームでサポートされています。
11.1.xx	SDX 14xxx、SDX 25xxx。注記: クリーンインストールオプションは、10Gのファクトリパーティションを持つ他のSDXプラットフォームでサポートされています。
11.1.51.x	すべてのSDXプラットフォーム。
12.1.xx	すべてのSDXプラットフォーム。
13.0.xx	すべてのSDXプラットフォーム。
13.1.xx	すべてのSDXプラットフォーム。

前提条件

以下を確認してください。

- すべてのプライマリ高可用性ノードを別のSDXアプライアンスにフェイルオーバーします。高可用性機能がない場合は、それに応じてダウンタイムを計画してください。
- シングルバンドルイメージをローカルマシンにダウンロードします。

重要:

クリーンインストールオプションを使用している間は、アプライアンスを再起動したり、電源を入れ直したりしないでください。アプライアンスは複数回再起動されます。

アプライアンスを単一のバンドルイメージバージョンにリセットする

1. **Configuration > System > System Administration** グループに移動します。
2. **Appliance Reset** をクリックします。
3. **Appliance Reset** ダイアログボックスで、**Reset Type** リストから **Clean Install** を選択します。
4. **OK** をクリックします。

外部認証サーバーのカスケーディング

複数の外部認証サーバーをカスケーディングすることで、外部ユーザーを認証および承認するための継続的で信頼性の高いプロセスが提供されます。最初の認証サーバーで認証が失敗した場合、管理サービスは2番目の外部認証サーバーを使用してユーザーの認証を試みます。

カスケーディング認証を有効にするには、外部認証サーバーを管理サービスに追加します。詳細については、「[外部認証の構成](#)」を参照してください。サポートされている外部認証サーバー（RADIUS、LDAP、TACACS）のいずれかのタイプを追加できます。たとえば、カスケーディング認証用に4つの外部認証サーバーを追加するには、RADIUS、LDAP、TACACSサーバーの任意の組み合わせを追加できます。また、同じタイプのサーバーを4つすべて追加することもできます。NetScaler Application Delivery Managementでは、最大32台の外部認証サーバーを構成できます。

注:

CLIを介した外部認証サーバーのカスケーディングはサポートされていません。

外部認証サーバーをカスケーディングする

1. **Configuration**タブの**System**で、**Authentication**を展開します。
2. **Authentication**ページで、**Authentication Configuration**をクリックします。
3. **Authentication Configuration**ページで、**Server Type**ドロップダウンリストから**EXTERNAL**を選択します（外部サーバーのみをカスケーディングできます）。
4. **Insert**をクリックし、開いた**External Servers**ページで、カスケーディングする認証サーバーを1つまたは複数選択します。
5. **OK**をクリックします。

選択したサーバーは、次の図に示すように**Authentication Servers**ページに表示されます。認証の順序を変更するには、サーバー名の横にあるアイコンを使用して、リスト内でサーバーを上下に移動します。



ユーザーのロックを解除する

NetScaler SDX管理者は、ロックアウト間隔が期限切れになる前にユーザーのロックを解除できます。ユーザーがコンソール経由でManagement Serviceにログインする場合、ロックアウトは適用されません。ロックアウト間隔も秒から分に変更されます。最小値 = 1分。最大値 = 30分。

GUIを使用してユーザーのロックを解除する

1. 構成 > システム > ユーザー管理 > ユーザーに移動します。
2. ロックを解除するユーザーを選択します。
3. ロック解除をクリックします。

CLIを使用してユーザーのロックを解除する

コマンドプロンプトで、次のように入力します。

```
set systemuser id=<ID> unlock=true
```

NetScalerインスタンスのプロビジョニング

注

NetScaler SDXアプライアンスをリリース13.1にインストールまたはアップグレードした後、NetScaler Consoleサービス接続はデフォルトで有効になっています。詳細については、「データガバナンス」および「NetScaler Consoleサービス接続」を参照してください。

Management Serviceを使用して、SDXアプライアンス上に1つ以上のNetScalerインスタンスをプロビジョニングできます。インストールできるインスタンスの数は、購入したライセンスによって異なります。追加されたインスタンスの数がライセンスで指定された数と等しい場合、Management Serviceはそれ以上のNetScalerインスタンスのプロビジョニングを許可しません。

注:

基盤となるハードウェアプラットフォームとは独立して、ネットワークインターフェイス上で最大20個のVPXインスタンスを構成できます。

SDXアプライアンス上でNetScaler VPXインスタンスをプロビジョニングするには、次の手順を実行します。

1. NetScalerインスタンスにアタッチする管理者プロファイルを定義します。このプロファイルは、Management ServiceがADCインスタンスをプロビジョニングし、その後インスタンスと通信して構成データを取得するために使用するユーザー資格情報を指定します。デフォルトの管理者プロファイルを使用することもできます。
2. .xvaイメージファイルをManagement Serviceにアップロードします。
3. Management Serviceの「NetScalerのプロビジョニング」ウィザードを使用してNetScalerインスタンスを追加します。Management Serviceは、NetScalerインスタンスをSDXアプライアンスに暗黙的に展開し、その後インスタンスの構成詳細をダウンロードします。

警告

インスタンスのプロビジョニングされたネットワークインターフェイスまたはVLANを変更する場合は、インスタンス上で直接変更を行うのではなく、Management Serviceを使用してください。

管理者プロファイルの作成

管理者プロファイルは、NetScalerインスタンスをプロビジョニングする際にManagement Serviceが使用するユーザー資格情報を指定します。これらの資格情報は、後でインスタンスと通信して構成データを取得する際に使用されます。管理者プロファイルで指定されたユーザー資格情報は、クライアントがCLIまたはGUIを介してNetScalerインスタンスにログオンする際にも使用されます。

管理者プロファイルを使用すると、Management ServiceとVPXインスタンスが相互にセキュアチャンネル経由またはHTTPを使用してのみ通信するように指定することもできます。

インスタンスのデフォルトの管理者プロファイルは、デフォルトの管理者ユーザー名を指定します。このプロファイルは変更または削除できません。ただし、インスタンスをプロビジョニングする際に、ユーザー定義の管理者プロファイルを作成し、それをインスタンスにアタッチすることで、デフォルトのプロファイルを上書きする必要があります。Management Service管理者は、NetScalerインスタンスにアタッチされていないユーザー定義の管理者プロファイルを削除できます。

重要

VPXインスタンスで直接パスワードを変更しないでください。そうすると、インスタンスはManagement Serviceから到達不能になります。パスワードを変更するには、まず管理者プロファイルを作成し、次にNetScalerインスタンスを変更して、管理者プロファイルリストからこのプロファイルを選択します。

高可用性セットアップでNetScalerインスタンスのパスワードを変更するには、まずセカンダリノードとして指定されたインスタンスのパスワードを変更します。次に、プライマリノードとして指定されたインスタンスのパスワードを変更します。パスワードはManagement Serviceを使用してのみ変更することを忘れないでください。

管理者プロファイルの作成

1. **Configuration**タブのナビゲーションペインで、**NetScaler Configuration**を展開し、**Admin Profiles**をクリックします。
2. **Admin Profiles**ペインで、**Add**をクリックします。
3. **Create Admin Profile**ダイアログボックスが表示されます。

管理者プロファイルSNMP(/en-us/sdx/media/admin-profile-snmp-v3-citrix.png)

次のパラメータを設定します。

- プロファイル名: 管理者プロファイルの名前。デフォルトのプロファイル名は **nsroot** です。ユーザー定義のプロファイル名を作成できます。
- パスワード: NetScalerインスタンスにログオンするために使用するパスワード。最大長: 31文字。
- SSHポート: SSHポートを設定します。デフォルトポートは22です。
- **NetScaler通信にグローバル設定を使用:** Management ServiceとNetScalerインスタンス間の通信設定をシステム設定で定義する場合は、これを選択します。このチェックボックスをオフにして、プロトコルをHTTPまたはHTTPSに変更できます。
 - Management ServiceとNetScalerインスタンス間の通信にHTTPプロトコルを使用するには、**http**オプションを選択します。
 - 管理サービスとNetScalerインスタンス間の通信にセキュアチャネルを使用するには、**https**オプションを選択します。

4\ **SNMP**でバージョンを選択します。v2を選択した場合は、手順5に進みます。v3を選択した場合は、手順6に進みます。

5\ SNMP v2で、SNMP **Community**名を追加します。

6\ SNMP v3で、**Security Name**と**Security Level**を追加します。

7\ **Timeout Settings**で、値を指定します。

8\ **Create**をクリックし、次に**Close**をクリックします。作成した管理者プロファイルが**Admin Profiles**ペインに表示されます。

Default列の値がtrueの場合、デフォルトプロファイルが管理者プロファイルです。値がfalseの場合、ユーザー定義プロファイルが管理者プロファイルです。

ユーザー定義の管理者プロファイルを使用しない場合は、管理サービスから削除できます。ユーザー定義の管理者プロファイルを削除するには、**Admin Profiles** ペインで削除するプロファイルを選択し、**Delete** をクリックします。

NetScaler .xva イメージをアップロードする

NetScaler VPX インスタンスを追加するには、.xva ファイルが必要です。

VPX インスタンスをプロビジョニングする前に、NetScaler SDX .xva ファイルを SDX アプライアンスにアップロードします。また、.xva イメージファイルをバックアップとしてローカルコンピューターにダウンロードすることもできます。.xva イメージファイルの形式は次のとおりです：

```
NSVPX-XEN-ReleaseNumber-BuildNumber_nc .xva。
```

NetScaler XVA Files ペインで、次の詳細を表示できます。

- **Name:** .xva イメージファイルの名前。ファイル名にはリリースとビルド番号が含まれます。たとえば、ファイル名 `NSVPX-XEN-12.1-56.22.xva.gz` はリリース 12.1 ビルド 56.22 を指します。
- **Last Modified:** .xva イメージファイルが最後に変更された日付。
- **Size:** .xva イメージファイルのサイズ（MB 単位）。

NetScaler .xva ファイルをアップロードするには

1. **Configuration** タブのナビゲーションペインで、**NetScaler Configuration** を展開し、**XVA Files** をクリックします。
2. **NetScaler XVA Files** ペインで、**Upload** をクリックします。
3. **Upload NetScaler instance XVA** ダイアログボックスで、**Browse** をクリックし、アップロードする XVA イメージファイルを選択します。
4. **Upload** をクリックします。アップロード後、XVA イメージファイルが **NetScaler XVA Files** ペインに表示されます。

NetScaler .xva ファイルをダウンロードしてバックアップを作成するには

1. **NetScaler Build Files** ペインで、ダウンロードするファイルを選択し、**Download** をクリックします。
2. **File Download** メッセージボックスで、**Save** をクリックします。
3. **Save As** メッセージボックスで、ファイルを保存する場所を参照し、**Save** をクリックします。

NetScaler インスタンスを追加する

Management Service から NetScaler インスタンスを追加する場合、いくつかのパラメータの値を指定する必要があります。Management Service は、これらの設定を NetScaler インスタンスに自動的に構成します。

SDX インスタンスの詳細(/en-us/sdx/media/sdx-instance-details-citrix.png)

- **名前:** NetScaler インスタンスに名前を割り当てます。
- SDX Management Service と VPX インスタンス間の独立した内部常時接続を有効にするには、**Manage through internal network** を選択します。この機能は、SDX アプライアンスで実行されている VPX インスタンスのバージョン 13.0-36.27 以降でサポートされています。
- 管理目的で NetScaler VPX インスタンスにアクセスするために、IPv4 アドレス、IPv6 アドレス、または IPv4 と IPv6 の両方のアドレスを選択します。NetScaler インスタンスは、管理 IP (NSIP) を1つしか持つことができません。NSIP アドレスを削除することはできません。
- IPアドレスにネットマスク、デフォルトゲートウェイ、およびManagement Serviceへのネクストホップを割り当てます。
- VPXがバージョン13.0–88.9または13.1–37.8以降でプロビジョニングされている場合、**ゲートウェイ**および**Management Serviceへのネクストホップ**フィールドは、以下のいずれかの条件下でオプションとなります。
 - **内部ネットワーク経由で管理**が有効になっている場合。
 - 設定されたIPv4アドレスがManagement ServiceのIPアドレスと同じサブネットにある場合。



次に、XVAファイル、管理者プロファイル、およびインスタンスの説明を追加します。

注: 高可用性セットアップ（アクティブ-アクティブまたはアクティブ-スタンバイ）の場合、Citrix は2つのNetScaler VPXインスタンスを異なるSDXアプライアンスに構成することを推奨します。セットアップ内のインスタンスが、CPU、メモリ、インターフェイス、1秒あたりのパケット数（PPS）、スループットなど、同一のリソースを持つことを確認してください。

ライセンスの割り当て

このセクションでは、NetScaler用に取得したライセンスを指定します。ライセンスは、Standard、Enterprise、Platinumのいずれかです。

注: アスタリスクは必須フィールドを示します。



帯域幅バースト機能が必要な場合は、**割り当てモード**で**バースト可能**を選択します。詳細については、「[SDXでの帯域幅メータリング](#)」を参照してください。

暗号化の割り当て

リリース12.1 48.13以降、暗号化容量を管理するインターフェイスが変更されました。詳細については、「[暗号化容量の管理](#)」を参照してください。

リソースの割り当て

SDXで実行されているVPXインスタンスの場合、デフォルトでは管理CPUは1つしかありません。リリース13.1ビルド53.x以降では、専用コアが2つ以上ある場合、VPXインスタンスをプロビジョニングまたは編集する際に、管理CPUをもう1つ追加できます。この機能を使用するには、SDXとVPXの両方がソフトウェアバージョン13.1-53.x以降である必要があります。

リソース割り当てで、合計メモリ、1秒あたりのパケット数、およびCPUを割り当てます。

追加の管理CPUを追加するには:

1. **CPU**リストから**専用 (2コア)** 以上を選択します。
2. **追加の管理CPUを追加オプション**を選択します。



CPU: インスタンスに専用コアを割り当てるか、インスタンスが他のインスタンスとコアを共有します。共有を選択した場合、1つのコアがインスタンスに割り当てられますが、リソースが不足している場合は、そのコアが他のインスタンスと共有される可能性があります。CPUコアが再割り当てされた場合は、影響を受けるインスタンスを再起動します。パフォーマンスの低下を避けるため、CPUコアが再割り当てされたインスタンスを再起動してください。

SDXリリース11.1.x.x (MR4) 以降、SDX 25000xxプラットフォームを使用している場合は、インスタンスに最大16コアを割り当てることができます。また、SDX 2500xxxプラットフォームを使用している場合は、インスタンスに最大11コアを割り当てることができます。

注:

- インスタンスの場合、設定できる最大スループットは180 Gbpsです。
- 最適なパフォーマンスを得るには、ライセンスに関係なく、パケットエンジン (PE) ごとに4 GBのメモリを割り当ててをお勧めします。たとえば、6つのPEを持つVPXには24 GBのメモリが割り当てられている必要があります。

次の表に、サポートされているVPX、シングルバンドルイメージバージョン、およびインスタンスに割り当て可能なコア数を示します。

プラットフォーム名	合計コア数	VPXプロビジョニング に利用可能な合計コア 数	単一インスタンスに割 り当て可能な最大コア 数
SDX 8015、SDX 8400、および SDX 8600	4	3	3
SDX 8900	8	7	7
SDX 11500、SDX 13500、SDX 14500、SDX 16500、SDX 18500、および SDX 20500	12	10	5
SDX 11515、SDX 11520、SDX 11530、SDX 11540、および SDX 11542	12	10	5
SDX 17500、SDX 19500、および SDX 21500	12	10	5
SDX 17550、SDX 19550、SDX 20550、および SDX 21550	12	10	5
SDX 14020、SDX 14030、SDX 14040、SDX 14060、SDX 14080、および SDX 14100	12	10	5

プラットフォーム名	合計コア数	VPXプロビジョニング に利用可能な合計コア 数	単一インスタンスに割 り当て可能な最大コア 数
SDX 22040、SDX 22060、SDX 22080、SDX 22100、および SDX 22120	16	14	7
SDX 24100 および SDX 24150	16	14	7
SDX 14020 40G、SDX 14030 40G、SDX 14040 40G、SDX 14060 40G、SDX 14080 40G、および SDX 14100 40G	12	10	10
SDX 14020 FIPS、SDX 14030 FIPS、SDX 14040 FIPS、SDX 14060 FIPS、SDX 14080 FIPS、および SDX 14100 FIPS	12	10	5
SDX 14040 40S、SDX 14060 40S、SDX 14080 40S、および SDX 14100 40S	12	10	10
SDX 25100A、25160A、25200A	20	18	9
SDX 25100-40G、25160-40G、25200-40G	20	18	16 (バージョンが 11.1-51.x以降の場合); 9 (バージョンが 11.1-50.x以前の場合; 11.0および10.5のすべてのバージョン)

プラットフォーム名	合計コア数	VPXプロビジョニング に利用可能な合計コア 数	単一インスタンスに割 り当て可能な最大コア 数
SDX 26100、 26160、26200、 26250	28	26	16
エスディーエックス 26100-50S, 26160-50S, 26200-50S, 26250-50S	28	26	16
エスディーエックス 26100-100G, 26160-100G, 26200-100G, 26250-100G	28	26	25
SDX 15000	16	14	14
SDX 15000-50G	16	14	14
SDX 9100	10	9	9
SDX 16000	32	30	16

注:

専有コアは、インスタンスで実行されているパケットエンジンの数に対応します。専有コアで作成されたVPXインスタンスの場合、管理用にCPUが追加で割り当てられます。

SDX上のNetScaler VPXで追加の管理CPUを有効にするための推奨されるプラクティス

NetScaler SDX展開では、各VPXインスタンスがデータプレーン（パケット処理）と管理プレーン（制御および管理操作）の両方のワークロードを処理します。管理アクティビティが高い環境では、管理プレーンでCPU競合が発生し、構成変更、監視、API操作などのタスクの応答性に影響を与える可能性があります。

システムのパフォーマンスと安定性を向上させるために、CitrixはSDXプラットフォームで実行されているNetScaler VPXインスタンスに対して、追加の管理CPU（追加の管理スレッドとも呼ばれます）を有効にすることを推奨しています。

概要

デフォルトでは、管理プレーンの処理は利用可能なハイパースレッドに分散され、パケットエンジン間でタイムシェアリングされます。NetScaler 13.1ビルド以降、SDXは管理プレーンタスク専用の追加の管理ハイパースレッドの有効化をサポートしています。

注：

NetScalerバージョン13.1ビルド63.16以降、VPXインスタンスに2つ以上の専用コアを選択すると、デフォルトで追加の管理CPUが割り当てられます。

主な特徴は次のとおりです。

- 追加の管理CPUは、物理コアではなくハイパースレッドを使用して実装されます。
- 管理プレーン操作に専用の処理能力を提供します。
- 他のプラットフォームで使用されている従来の追加管理CPU実装とは異なります。

利点：

- 管理プレーンの応答性の向上
 - CLIおよびAPIコマンドの実行速度の向上。
 - 構成変更の遅延の削減。
 - GUIおよび自動化ワークフローの応答性の向上。
- 安定性の向上
 - 負荷がかかった状態での管理プレーンの競合の可能性を低減します。
 - 高度な監視、ログ記録、または自動化アクティビティの影響を最小限に抑えます。
- データプレーンのパフォーマンスに影響なし
 - パケット処理コア（パケットエンジン）は削減されたり、影響を受けたりしません。
 - データプレーンのスループットは変更されません。

前提条件：

追加の管理CPUを有効にする前に、以下の前提条件が満たされていることを確認してください。

- **NetScalerバージョン:** SDXおよびVPXインスタンスの両方でNetScaler 13.1-63.x以降。
- **VPXプロビジョニング:** 各VPXインスタンスに少なくとも2つのCPUコアを割り当てる必要があります。
- **プラットフォーム要件:** SDXプラットフォームでハイパースレッディングを有効にする必要があります。

追加の管理CPUを有効にするタイミング

Citrixは、お使いの環境で以下のいずれかの状況が見られる場合に、追加の管理CPUを有効にすることをお勧めします。

高い管理アクティビティ	パフォーマンスに関する懸念
継続的な監視とテレメトリ収集	CLIまたはGUIの応答時間の遅延
頻繁な構成変更または自動化	構成の適用における遅延
高いAPIまたはオーケストレーションアクティビティ	高い管理CPU使用率

注:

管理CPUに負荷がかかっている場合は、この機能を有効にしてください。

運用上の考慮事項:

- 追加の管理CPUを有効または無効にした後、VPXの再起動が必要です。
- 追加の管理CPUの動作は、NetScaler MPXおよびハイパーバイザー上のNetScaler VPXとは異なります。
- この機能は、SDX上で実行されているVPXインスタンスに特化して適用されます。

推奨事項の概要:

- 追加の管理CPUを有効にすることは、推奨される低リスクの構成です。
- これにより、管理プレーンのパフォーマンスと信頼性が向上します。
- データプレーンのスループットやパケットエンジンの割り当てには影響しません。
- ほとんどのSDX展開において、ベストプラクティスと見なされています。

インスタンス管理

Instance Administration の下にある **Add Instance Administration** を選択して、VPX インスタンスの管理者ユーザーを作成できます。

インスタンス管理者(/en-us/sdx/media/instance-admin-citrix.png)

次の詳細を追加します。

ユーザー名: NetScaler インスタンス管理者のユーザー名。このユーザーはスーパーユーザーアクセス権を持っていますが、VLAN とインターフェイスを設定するためのネットワークコマンドへのアクセス権はありません。

パスワード: ユーザー名のパスワード。

Shell/Sftp/Scp アクセス: NetScaler インスタンス管理者に許可されるアクセス。このオプションはデフォルトで選択されています。

ネットワーク設定

- **L2 モードを許可:** NetScaler インスタンスで L2 モードを許可できます。**Networking Settings** の下にある **Allow L2 Mode** を選択します。インスタンスにログオンして L2 モードを有効にする前に。詳細については、「[NetScaler インスタンスでの L2 モードの許可](#)」を参照してください。

ネットワーク設定(/en-us/sdx/media/network-settings-citrix.png)

注:

- Management Service からインスタンスの L2 モードを無効にする場合は、そのインスタンスにログオンして L2 モードを無効にする必要があります。そうしないと、インスタンスを再起動した後に他のすべての NetScaler モードが無効になる可能性があります。
- ADC インスタンスが SDX にプロビジョニングされた後、ADC インスタンスからインターフェイスまたはチャンネルを削除することはできません。ただし、ADC インスタンスにインターフェイスまたはチャンネルを追加することはできます。

- **インターフェイス 0/1 および 0/2:** デフォルトでは、管理 LA にインターフェイス 0/1 および 0/2 が選択されています。

- **VLAN タグ:** 管理インターフェイスの VLAN ID を指定します。次に、データインターフェイスを追加します。

注

インスタンスに追加するインターフェイスのインターフェイスIDは、SDXアプライアンスの物理インターフェイス番号と必ずしも一致しません。インスタンス1に関連付ける最初のインターフェイスがインターフェイス1/4の場合、インスタンスのインターフェイス設定を表示するとインターフェイス1/1として表示されます。番号が変更されるのは、それがインスタンス1に関連付けた最初のインターフェイスであるためです。



- **タグなしトラフィックを許可:** 「タグなしトラフィックを許可」チェックボックスをオンにして、NetScalerインスタンスがタグなしトラフィックを処理できるようにします。

注:

SDXアプライアンスのバージョンが13.1-24.x以降で、NetScalerインスタンスのバージョンが13.1-24.xより前の場合、「タグなしトラフィックを許可」チェックボックスがオフになっていても、ADCインスタンスはMellanoxインターフェイス上のタグなしトラフィックを処理します。

- **許可されたVLAN:** NetScalerインスタンスに関連付けることができるVLAN IDのリストを指定します。
- **MACアドレスモード:** MACアドレスを割り当てます。次のいずれかのオプションを選択します。
 - **デフォルト:** Citrix Hypervisor™がMACアドレスを割り当てます。
 - **カスタム:** 生成されたMACアドレスを上書きするMACアドレスを指定するには、このモードを選択します。
 - **生成済み:** 以前に設定されたベースMACアドレスを使用してMACアドレスを生成します。ベースMACアドレスの設定については、「インターフェイスへのMACアドレスの割り当て」を参照してください。
- **VMAC設定 (仮想MACを設定するためのIPv4およびIPv6 VRID)**

- **VRID IPv4:** VMACを識別するIPv4 VRID。指定可能な値: 1～255。詳細については、「インターフェースでのVMACの構成」を参照してください。
- **VRID IPv6:** VMACを識別するIPv6 VRID。指定可能な値: 1～255。詳細については、「インターフェースでのVMACの構成」を参照してください。

管理VLAN設定

通常、管理サービスとVPXインスタンスの管理アドレス（NSIP）は同じサブネットワークにあり、通信は管理インターフェースを介して行われます。ただし、管理サービスとインスタンスが異なるサブネットワークにある場合は、VPXインスタンスをプロビジョニングする際にVLAN IDを指定する必要があります。このIDは、インスタンスが起動時にネットワーク経由で到達可能であるために必要です。デプロイメントでNSIPがVPXインスタンスのプロビジョニング時に選択されたインターフェースからのみアクセス可能である必要がある場合は、NSVLANオプションを選択します。

NSVLANオプションが選択されている場合、NetScalerインスタンスをプロビジョニングした後は、この設定を変更できません。



注：

- HAハートビートは、NSVLANの一部であるインターフェースでのみ送信されます。
- NSVLANは、VPX XVAビルド9.3 53.4以降でのみ構成できます。

重要： NSVLANが選択されていない場合、VPXインスタンスで「clear config full」コマンドを実行すると、VLAN構成が削除されます。

完了をクリックして、NetScaler VPXアプライアンスをプロビジョニングします。

NetScalerインスタンスの変更

プロビジョニングされたADCインスタンスのパラメータ値を変更するには、**NetScaler**インスタンスペインで、変更するインスタンスを選択し、**変更**をクリックします。ADC変更ウィザードで、パラメータを変更します。

注：

- VPXインスタンスを編集して管理CPUを1つ追加できるのは、2つ以上の専用コアがあり、VPXとSDXの両方がリリース13.1およびビルド53.x以降である場合のみです。
- リリース13.1-53.xより前のVPXで**追加の管理CPUを追加オプション**を選択すると、エラーが発生します。この機能を使用するには、VPXインスタンスをリリース13.1-53.x以降にアップグレードしてください。
- VPXインスタンスを13.1-53.xより前のビルドにダウングレードする前に、**追加の管理CPUを追加オプション**を無効にする必要があります。そうしないと、VPXインスタンスのパフォーマンスに影響が出ます。
- **追加の管理CPUを追加オプション**が無効になっておらず、VPXインスタンスが13.1-53.xより前のバージョンにダウングレードされた場合、アラームが生成されます。

注意点:

- SSLチップの数、インターフェイス、メモリ、機能ライセンスなどのパラメータを変更すると、NetScalerインスタンスはこれらのパラメータを有効にするために暗黙的に停止し、再起動します。
- イメージおよびユーザー名のパラメータは変更できません。
- インターフェイスまたはチャンネルをADCインスタンスから削除することはできません。ただし、新しいインターフェイスまたはチャンネルをADCインスタンスに追加することはできます。
- SDXアプライアンスにプロビジョニングされたADCインスタンスを削除するには、**NetScaler** インスタンスペインで、削除するインスタンスを選択し、**削除**をクリックします。**確認**メッセージボックスで、**はい**をクリックしてNetScalerインスタンスを削除します。

VLANを特定の仮想インターフェイスに制限する

SDXアプライアンス管理者は、NetScalerインスタンスに関連付けられた仮想インターフェイスに特定の802.1Q VLANを強制できます。この機能は、インスタンス管理者による802.1Q VLANの使用を制限するのに特に役立ちます。異なる2つの会社には属する2つのインスタンスがSDXアプライアンスでホストされている場合、2つの会社が同じVLAN IDを使用することを制限できます。これにより、一方の会社は他方の会社のトラフィックを見ることがなくなります。インスタンス管理者がインターフェイスを802.1Q VLANに割り当てようとすると、指定されたVLAN IDが許可リストの一部であることを確認するための検証が実行されます。

デフォルトでは、任意のVLAN IDをインターフェイスで使用できます。インターフェイス上のタグ付きVLANを制限するには、NetScalerインスタンスのプロビジョニング時にネットワーク設定でVLAN IDを指定します。後でインスタンスを変更して指定することもできます。範囲を指定するには、ハイフンでIDを区切ります（例: 10–12）。最初にいくつかのVLAN IDを指定したが、後でそれらすべてを許可リストから削除した場合、そのインターフェイスで任意のVLAN IDを使用できます。実質的に、デフォルト設定に戻したことになります。

許可されたVLANのリストを作成した後、SDX管理者はVLANを作成するためにインスタンスにログオンする必要はありません。管理者は、管理サービスから特定のインスタンスのVLANを追加および削除できます。

重要: L2モードが有効になっている場合、管理者は異なるNetScalerインスタンス上のVLAN IDが重複しないように注意する必要があります。

許可されたVLAN IDを指定するには

1. ADCプロビジョニングウィザードまたはADC変更ウィザードの「ネットワーク設定」ページで、**許可されたVLAN**に、このインターフェイスで許可される1つ以上のVLAN IDを指定します。範囲を指定するにはハイフンを使用します。例: 2–4094。
2. ウィザードの指示に従います。
3. **完了**をクリックし、**閉じる**をクリックします。

管理サービスからインスタンスのVLANを構成するには

1. 「**Configuration**」タブで、NetScaler > Instances に移動します。
2. インスタンスを選択し、「**VLAN**」をクリックします。
3. 詳細ペインで、「**Add**」をクリックします。
4. 「**Create NetScaler VLAN**」ダイアログボックスで、次のパラメータを指定します。
 - **VLAN ID** — 特定のフレームが属するVLANを一意に識別する整数。NetScalerは最大4094のVLANをサポートします。ID 1はデフォルトVLAN用に予約されています。
 - **IPv6ダイナミックルーティング** — このVLANで、すべてのIPv6ダイナミックルーティングプロトコルを有効にします。

注: 「**ENABLED**」設定を機能させるには、インスタンスにログオンし、VTYSHコマンドラインからIPv6ダイナミックルーティングプロトコルを設定する必要があります。

5. VLANの一部となる必要があるインターフェイスを選択します。
6. 「**Create**」をクリックし、「**Close**」をクリックします。

暗号容量の管理

リリース 12.1 48.13 以降、暗号容量を管理するインターフェイスが変更されました。

Management Service は、NetScaler SDX アプライアンス上の SSL 容量を示すために、非対称暗号ユニット (ACU)、対称暗号ユニット (SCU)、および暗号仮想インターフェイスを提供します。以前は、暗号容量は SSL チップ、SSL コア、および SSL 仮想機能の単位で割り当てられていました。レガシー SSL チップが ACU および SCU ユニットのどのように変換されるかについての詳細は、[レガシー SSL チップから ACU および SCU への変換テーブル](#) を参照してください。

Management Service GUI を使用して、ACU および SCU 単位で NetScaler VPX インスタンスに暗号容量を割り当てることができます。

次の表は、ACU、SCU、および暗号仮想インスタンスに関する簡単な説明を示しています。

表。ユニット暗号ユニット

新しい暗号ユニット	説明
非対称暗号ユニット (ACU)	1 ACU = (RSA) 2 K (2048 ビット鍵サイズ) 復号化の 1 秒あたりの操作数 (ops)。詳細については、 ACU から PKE リソースへの変換テーブル を参照してください。
対称暗号ユニット (SCU)	1 SCU = AES-128-CBC + SHA256-HMAC @ 1024B の 1 Mbps。この定義は、すべての SDX プラットフォームに適用されます。
暗号仮想インターフェイス	仮想機能とも呼ばれる暗号仮想インターフェイスは、SSL ハードウェアの基本単位を表します。これらのインターフェイスが使い果たされると、SSL ハードウェアを VPX インスタンスにさらに割り当てることはできません。暗号仮想インターフェイスは読み取り専用エンティティであり、SDX アプライアンスはこれらのエンティティを自動的に割り当てます。

SDX アプライアンスの暗号容量を表示する

SDX GUI のダッシュボードで、SDX アプライアンスの暗号容量を表示できます。ダッシュボードには、SDX アプライアンスで使用中および利用可能な ACU、SCU、および仮想インターフェイスが表示されます。暗号容量を表示するには、**ダッシュボード > 暗号容量**に移動します。



VPXインスタンスのプロビジョニング中に暗号容量を割り当てる

SDXアプライアンスでVPXインスタンスをプロビジョニングする際、**暗号割り当て**の下で、VPXインスタンスのACUとSCUの数を割り当てることができます。VPXインスタンスのプロビジョニング手順については、「NetScalerインスタンスのプロビジョニング」([/ja-jp/sdx/13-1/provision-netscaler-instances.html](#))を参照してください。

VPXインスタンスのプロビジョニング中に暗号容量を割り当てるには、次の手順に従います。

1. Management Serviceにログオンします。
2. **Configuration > NetScaler > Instances**に移動し、**Add**をクリックします。
3. **暗号割り当て**の下で、利用可能なACU、SCU、および暗号仮想インターフェイスを表示できます。ACUとSCUの割り当て方法は、SDXアプライアンスによって異なります。
 - a. 「異なるSDXアプライアンスで利用可能なACUカウンターの最小値」(#minimum-value-of-an-acu-counter-available-for-different-sdx-appliances)に記載されているアプライアンスの場合、指定された数値の倍数でACUを割り当てることができます。SCUは自動的に割り当てられ、SCU割り当てフィールドは編集できません。そのモデルで利用可能な最小ACUの倍数でACU割り当てを増やすことができます。たとえば、最小ACUが4375の場合、ACUの増分は8750、13125などになります。

例。 SCUが自動的に割り当てられ、ACUが指定された数値の倍数で割り当てられる暗号割り当て。



異なるSDXアプライアンスで利用可能なACUカウンターの最小値

SDXプラットフォーム	ACUカウンターの最小値
22040、22060、22080、22100、22120、 24100、24150 (36ポート	2187

SDXプラットフォーム	ACUカウンターの最小値
8400, 8600, 8010, 8015	2812
17500, 19500, 21500	2812
17550, 19550, 20550, 21550	2812
11500, 13500, 14500, 16500, 18500, 20500	2812
11515, 11520, 11530, 11540, 11542	4375
14xxx	4375
14xxx 40エス	4375
14xxx 40ジー	4375
14xxx FIPS	4375
25xxx	4375
25xxx A型	4575

b. 前の表に記載されていないその他のSDXプラットフォームでは、ACUとSCUを自由に割り当てるができます。SDXアプライアンスは、暗号仮想インターフェイスを自動的に割り当てます。

例。ACUとSCUの両方が自由に割り当てられる暗号割り当て



4./ VPXインスタンスをプロビジョニングするためのすべての手順を完了し、完了をクリックします。詳細については、「[NetScalerインスタンスのプロビジョニング](#)」を参照してください。

暗号ハードウェアの健全性を表示

Management Serviceでは、SDXアプライアンスに付属する暗号ハードウェアの健全性を表示できます。暗号ハードウェアの健全性は、暗号デバイスと暗号仮想機能として表されます。暗号ハードウェアの健全性を表示するには、**ダッシュボード > リソース**に移動します。



注意事項

SDXアプライアンスを最新バージョンにアップグレードする際は、以下の点に注意してください。

- SDXユーザーインターフェイスのみがアップグレードされ、アプライアンスのハードウェア容量は同じままです。
- 暗号割り当てメカニズムは同じままであり、SDX GUIでの表示のみが変更されます。
- 暗号インターフェイスは下位互換性があり、NITROインターフェイスを使用してSDXアプライアンスを管理する既存の自動化メカニズムには影響しません。
- SDXアプライアンスのアップグレード後も、既存のVPXインスタンスに割り当てられた暗号は変更されません。管理サービスでの表示のみが変更されます。

ACUからPKEリソースへの変換テーブル

SDXプラットフォーム フォーム	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
22040、 22060、 22080、 22100、 22120、 24100、 24150 (36ポート)	2187	12497	2187	312	256	190
8400, 8600, 8010, 8015	2812	17000	2812	424	330	該当なし
11515, 11520, 11530, 11540, 11542	4375	25000	4375	625	512	381
22040, 22060,	4375	25000	4375	625	512	381

SDXプラットフォーム	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
22080,22100,22120 (24ポート)						
17500,19500,21500	2812	17000	2812	424	330	N/A
17550,19550,20550,21550	2812	17000	2812	424	330	N/A
11500,13500,14500,16500,18500,20500	2812	17000	2812	424	330	N/A
14000,14000-40G, 25000,25000A	4375	25000	4375	625	512	381
14000 FIPS	4375	25000	4375	625	512	381
14000-40S	4375	25000	4375	625	512	381
*8900 (8910,8920,8930)	1000	4615	1000	136	397	494
*9100 (9110,	1000	4615	1000	136	397	494

SDXプラットフォーム	ACU	RSA-RSA1K	RSA-RSA2K	RSA-RSA4K	ECDHE-RSA	ECDHE-ECDSA
9120, 9130)						
*26000-100G (26100, 26160, 26200 および 26250)	1000	4615	1000	136	397	494
*15000	1000	4615	1000	136	397	494
*15000-50G	1000	4615	1000	136	397	494
*16000	1000	4615	1000	136	397	494
*26000-50S	1000	4615	1000	136	397	494

*これらのプラットフォームでは、PKE の数値は最小保証値です。

ACU から PKE へのリソース変換表の読み方

ACU から PKE へのリソース変換表は、以下の点に基づいています。

- マネジメントサービスは、各VPXに暗号リソースの割り当てを支援します。マネジメントサービスは、パフォーマンスを割り当てたり、保証したりすることはできません。
- 実際のパフォーマンスは、パケットサイズ、使用される暗号/Keyex/HMAC（またはそのバリエーション）などによって異なります。

次の例は、ACUからPKEリソースへの変換テーブルの読み方と適用方法を理解するのに役立ちます。

例。 SDX 22040プラットフォームにおけるACUからPKEリソースへの変換

SDX 22040プラットフォーム上のVPXインスタンスに2187 ACUを割り当てると、256のECDHE-RSA操作または2187のRSA-2K操作などに相当する暗号リソースが割り当てられます。

レガシーSSLチップからACUおよびSCUへの変換テーブル

レガシーSSLチップがACUおよびSCUに変換される方法の詳細については、次の表を参照してください。

[ACUおよびSCU変換テーブル](#)

サードパーティ製仮想マシンのプロビジョニング

警告:

NetScaler SDX GUIでは、バージョン13.1ビルド37.x以降、「サードパーティインスタンス」のサポートは非推奨です。サードパーティインスタンスを引き続き使用する場合は、Citrixは以下の操作を実行することを推奨します。

- Management Serviceシェルにログオンします。
- ディレクトリ `/mpsconfig` にファイル `.thirdPartyVM` を作成します。
- `svmd restart` コマンドを実行してManagement Serviceを再起動します。

SDXアプライアンスは、以下のサードパーティ製仮想マシン（インスタンス）のプロビジョニングをサポートしています。

- SECUREMATRIX GSB
- インタースキャン ウェブセキュリティ
- ウェブセンス プロテクター
- ブルーキャット DNS/DHCP サーバー
- CA アクセス ゲートウェイ
- パロアルト VMシリーズ

SECUREMATRIX GSBは、トークンデバイスを持ち運ぶ必要のない、非常に安全なパスワードシステムを提供します。Websense Protectorは、監視およびブロック機能を提供し、機密情報のデータ損失や漏洩を防ぎます。BlueCat DNS/DHCP Serverは、ネットワークにDNSとDHCPを提供します。NetScaler SDX上のPaloAlto VM-Seriesは、高度なセキュリティ機能とADC機能を単一プラットフォームに統合し、企業およびサービスプロバイダーの顧客によるアプリケーションへの安全で信頼性の高いアクセスを可能にします。NetScaler SDX上のVM-Seriesの組み合わせは、Citrix Virtual Apps and Desktopsの展開向けに、完全に検証済みの安全なADCソリューションも提供します。

Management Serviceからインスタンスをプロビジョニング、監視、管理、トラブルシューティングできます。上記のすべてのサードパーティインスタンスは、Management Serviceと通信するために **SDXTools** デーモンを使用します。このデーモンは、プロビジョニングされたインスタンスにプリインストールされています。新しいバージョンが利用可能になったときに、デーモンをアップグレードできます。

サードパーティ製仮想マシンを設定すると、チャンネルの一部であるSR-IOVインターフェース (1/x および 10/x) は、インターフェースのリストに表示されません。チャンネルはサードパーティ製仮想マシンではサポートされていないため、インターフェースが表示されません。

注:

SDXアプライアンスにプロビジョニングできるインスタンスの総数は、アプライアンスにインストールされているライセンスによって異なります。

重要: サードパーティ製インスタンスをインストールする前に、Citrix Hypervisorのバージョンを 6.1.0 にアップグレードする必要があります。

SECUREMATRIX GSB

SECUREMATRIXは、使いやすく費用対効果の高い、高度に安全なトークンレスのワンタイムパスワード (OTP) 認証ソリューションです。マトリックス表からの位置、シーケンス、および画像パターンを組み合わせ使用し、1回限りのパスワードを生成します。SECUREMATRIX GSBサーバーとSECUREMATRIX認証サーバーは、VPN/SSL-VPNエンドポイント、クラウドベースのアプリケーションとリソース、デスクトップ/仮想デスクトップログイン、およびWebアプリケーション (OTP付きリバースプロキシ) のセキュリティを大幅に強化します。PC、仮想デスクトップ、タブレット、スマートフォンと互換性のあるソリューションを提供します。

ソフトウェア定義ネットワークでNetScaler SDXマルチテナントプラットフォームアーキテクチャを利用することで、SECUREMATRIXの強力な認証機能を、Web Interface、Citrix Virtual Apps and Desktops、および認証を必要とする他の多くのアプリケーションサービスなど、NetScalerを介して提供される他のテナントまたはクラウドサービスと統合できます。

SECUREMATRIX GSBインスタンスをプロビジョニングする

SECUREMATRIX GSBには、SDXアプライアンスの外部で構成する必要があるSECUREMATRIX認証サーバーが必要です。インターフェイスを1つだけ選択し、そのインターフェイスのネットワーク設定のみを指定します。

注: チャンネルの一部であるSR-IOVインターフェイス (1/xおよび10/x) は、インターフェイスのリストには表示されません。チャンネルはSECUREMATRIX GSBインスタンスではサポートされていません。

インスタンスのプロビジョニングを開始する前に、SECUREMATRIX WebサイトからXVAイメージをダウンロードし、SDXアプライアンスにアップロードします。XVAイメージのダウンロードの詳細については、SECUREMATRIX Webサイトを参照してください。SDXアプライアンスでManagement Serviceビルド118.7以降を使用していることを確認してください。

構成タブで、SECUREMATRIX GSB > ソフトウェアイメージに移動します。

XVAイメージをSDXアプライアンスにアップロードするには:

1. 詳細ペインで、**XVAファイル > アクション**の下にある**アップロード**をクリックします。
2. 表示されるダイアログボックスで、**参照**をクリックし、アップロードするXVAファイルを選択します。
3. **アップロード**をクリックします。XVAファイルがXVAファイルペインに表示されます。

SECUREMATRIXインスタンスをプロビジョニングするには

1. **構成タブで、SECUREMATRIX GSB > インスタンスに移動します。**
2. 詳細ペインで、**追加**をクリックします。
3. 「**Provision SECUREMATRIX GSB ウィザード**」で、画面の指示に従います。
4. 「**Finish**」をクリックし、次に「**Close**」をクリックします。

インスタンスをプロビジョニングした後、インスタンスにログオンし、詳細な構成を実行します。

プロビジョニングされたSECUREMATRIXインスタンスの設定を変更するには、**SECUREMATRIX Instances**ペインで、変更するインスタンスを選択し、**Modify**をクリックします。Modify SECUREMATRIX GSBウィザードで、パラメータを変更します。

注: インターフェイスパラメータまたはインスタンスの名前を変更すると、変更を有効にするためにインスタンスが停止して再起動します。

テクニカルサポートに提出するためのtarアーカイブを生成します。テクニカルサポートファイルの生成については、[テクニカルサポート用のTarアーカイブの生成](#)を参照してください。

SECUREMATRIX GSBインスタンスの構成をバックアップし、後でバックアップデータを使用してSDXアプライアンス上のインスタンスの構成を復元します。インスタンスのバックアップと復元については、[SDXアプライアンスの構成データのバックアップと復元](#)を参照してください。

SECUREMATRIX GSBインスタンスを監視する

SDXアプライアンスは、SECUREMATRIX GSBインスタンスの統計情報（SDXTools のバージョン、SSHおよびCRONデーモンの状態、Webサーバーの状態など）を収集します。

SECUREMATRIX GSBインスタンスに関連する統計情報を表示するには：

1. **SECUREMATRIX GSB > Instances**に移動します。
2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

SECUREMATRIX GSBインスタンスを管理する

Management ServiceからSECUREMATRIX GSBインスタンスを起動、停止、再起動、強制停止、または強制再起動できます。

Configurationタブで、**SECUREMATRIX GSB**を展開します。

インスタンスを起動、停止、再起動、強制停止、または強制再起動するには：

1. インスタンスをクリックします。
2. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。
 - 起動
 - シャットダウン
 - 再起動
 - 強制シャットダウン
 - 強制再起動
3. 確認メッセージボックスで、**はい**をクリックします。

SECUREMATRIX GSBインスタンスのSDXツールファイルをアップグレードする

SDXTools は、SECUREMATRIX GSBインスタンスで実行されているデーモンであり、管理サービスとインスタンス間の通信に使用されます。

SDXTools のアップグレードには、ファイルをSDXアプライアンスにアップロードし、インスタンスを選択した後に **SDXTools** をアップグレードする作業が含まれます。クライアントコンピューターからSDXアプライアンスに **SDXTools** ファイルをアップロードできます。

SDXToolsファイルをアップロードするには：

1. ナビゲーションペインで、**管理サービス**を展開し、**SDXToolsファイル**をクリックします。
2. 詳細ペインで、**アクション**リストから**アップロード**を選択します。
3. 「**SDXToolsファイルのアップロード**」ダイアログボックスで、「**参照**」をクリックし、ファイルを含むフォルダーに移動して、ファイルをダブルクリックします。
4. 「**アップロード**」をクリックします。

SDXToolsをアップグレードするには：

「**構成**」タブで、「**SECUREMATRIX GSB**」を展開します。

1. 「**インスタンス**」をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. 「**アクション**」リストから、「**SDXToolsのアップグレード**」を選択します。
4. 「**SDXToolsのアップグレード**」ダイアログボックスで、ファイルを選択し、「**OK**」をクリックしてから「**閉じる**」をクリックします。

SECUREMATRIX GSBインスタンスのアップグレードとダウングレード

SECUREMATRIX GSBインスタンスをアップグレードするプロセスには、ターゲットビルドのソフトウェアイメージをSDXアプライアンスにアップロードし、その後インスタンスをアップグレードすることが含まれます。ダウングレードでは、インスタンスの以前のバージョンがロードされます。

「**構成**」タブで、「**SECUREMATRIX GSB**」を展開します。

ソフトウェアイメージをアップロードするには：

1. 「**ソフトウェアイメージ**」をクリックします。
2. 詳細ペインで、「**アクション**」リストから「**アップロード**」を選択します。
3. ダイアログボックスで、「**参照**」をクリックし、ビルドファイルを含むフォルダーに移動して、ビルドファイルをダブルクリックします。
4. 「**アップロード**」をクリックします。

インスタンスをアップグレードするには：

1. 「**インスタンス**」をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. **アクション**リストから、**アップグレード**を選択します。

4. 表示されるダイアログボックスで、ファイルを選択し、**OK**をクリックし、**閉じる**をクリックします。

インスタンスをダウングレードするには：

1. 「**インスタンス**」をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. **アクション**リストから、**ダウングレード**を選択します。
4. 確認メッセージボックスで、**はい**をクリックします。

SECUREMATRIX GSBインスタンスのトラブルシューティング

Management ServiceからSECUREMATRIX GSBインスタンスにpingを実行し、デバイスに到達可能かどうかを確認します。Management Serviceからインスタンスへのパケットのルートをトレースして、インスタンスに到達するまでにかかるホップ数を特定できます。

インスタンスを再検出して、インスタンスの最新の状態と構成を表示します。再検出中に、Management Serviceは、SDXアプライアンスで実行されているSECUREMATRIX GSBの構成とバージョンを取得します。デフォルトでは、Management Serviceは30分ごとにインスタンスの再検出をスケジュールします。

構成タブで、**SECUREMATRIX GSB**を展開します。

インスタンスをpingするには:

1. **インスタンス**をクリックします。
2. 詳細ペインで、pingするインスタンスを選択し、**アクション**リストから**Ping**をクリックします。Pingメッセージボックスに、pingが成功したかどうかが表示されます。

インスタンスのルートをトレースするには:

1. **インスタンス**をクリックします。
2. 詳細ペインで、ルートをトレースするインスタンスを選択し、**アクション**リストから**TraceRoute**をクリックします。Tracerouteメッセージボックスに、インスタンスへのルートが表示されます。

インスタンスを再検出するには:

1. **インスタンス**をクリックします。
2. 詳細ペインで、再検出するインスタンスを選択し、**アクション**リストから**再検出**をクリックします。

3. 確認メッセージボックスで、**はい**をクリックします。

トレンドマイクロ InterScan Web Security

トレンドマイクロ InterScan Web Securityは、インターネットゲートウェイで従来のWeb脅威と新たなWeb脅威から動的に保護するソフトウェア仮想アプライアンスです。アプリケーション制御、アンチマルウェアスキャン、リアルタイムWebレピュテーション、柔軟なURLフィルタリング、高度な脅威保護を統合しています。その結果、優れた保護と、ネットワーク上でのクラウドベースアプリケーションの利用増加に対するより高い可視性と制御を提供します。リアルタイムレポートと集中管理により、管理者はプロアクティブな意思決定ツールを利用でき、その場でのリスク管理が可能になります。

インタースキャン ウェブセキュリティ：

- エンドユーザーのインターネットアクティビティに対するより深い可視性を可能にします
- 最大限の制御のために管理を集中化します
- Webの使用状況をリアルタイムで監視します
- その場での修復を可能にします
- アプライアンスの乱立とエネルギーコストを削減します
- オプションでデータ損失防止とサンドボックス実行分析を提供します

InterScan Web Securityインスタンスをプロビジョニングする前に、トレンドマイクロのWebサイトからXVAイメージをダウンロードする必要があります。XVAイメージをダウンロードしたら、NetScaler SDXアプライアンスにアップロードします。

注: チャンネルの一部であるSR-IOVインターフェイス (1/xおよび10/x) は、インターフェイスのリストに表示されません。チャンネルはInterScan Web Securityインスタンスではサポートされていません。

XVAイメージをSDXアプライアンスにアップロードするには:

1. **Configuration**タブから、**TrendMicro IWSVA > Software Images**に移動します。
2. 詳細ペインで、**XVA Files**タブの下にある**Upload**をクリックします。
3. 表示されるダイアログボックスで、**Browse**をクリックし、アップロードするXVAファイルを選択します。
4. 「**アップロード**」をクリックします。XVAファイルが「XVAファイル」ペインに表示されます。

TrendMicro IWSVAインスタンスをプロビジョニングするには：

1. 「構成」タブで、「TrendMicro IWSVA > インスタンス」に移動します。
2. 詳細ペインで、「追加」をクリックします。
3. 「TrendMicro IWSVAのプロビジョニング」ウィザードで、画面の指示に従います。
4. 「OK」をクリックし、その後「閉じる」をクリックします。

インスタンスをプロビジョニングした後、インスタンスにログオンし、詳細な構成を実行します。

プロビジョニングされたインスタンスのパラメータの値を変更するには、詳細ペインで、変更するインスタンスを選択し、その後「編集」をクリックします。「TrendMicro IWSVAの変更」ウィザードで、環境に適した値にパラメータを設定します。

ウェブセンス プロテクター

Websense (現在はForcepointとして知られている) Data Securityプロテクターは、アウトバウンド HTTPトラフィック (投稿) を傍受する仮想マシンです。その後、データ損失やウェブ上での機密データの漏洩を防ぐためにトラフィックを分析します。プロテクターは、DLPポリシー情報のために専用のWindowsサーバーと通信し、一致が検出された場合にデータが投稿されるのを監視またはブロックできます。コンテンツ分析はボックス内で実行されるため、このプロセス中に機密データがプロテクターから離れることはありません。

プロテクターのデータ損失防止 (DLP) 機能を使用するには、以下を実行します。

- Websense Data Security を購入してインストールします
- Data Security マネージャーで Web DLP ポリシーを構成します
- Management Service を介して初期設定を実行します。

Websense Protector インスタンスをプロビジョニングする

Websense Protector には、SDXアプライアンスの外部で構成する必要があるData Security Management Serverが必要です。管理インターフェイスを1つ、データインターフェイスを2つ正確に選択します。データインターフェイスには、を選択する必要があります。Data Security Management Server がWebsenseプロテクターの管理ネットワークを介してアクセスできることを確認してください。ネームサーバーには、このプロテクターにサービスを提供するドメインネームサーバー (DNS) のIPアドレスを入力します。

注: チャンネルの一部であるSR-IOVインターフェイス (1/x および 10/x) は、インターフェイスのリストには表示されません。チャンネルはWebsenseプロテクターインスタンスではサポートされていません。

インスタンスのプロビジョニングを開始する前に、Websenseウェブサイトからプロテクターイメージをダウンロードし、SDXアプライアンスにアップロードしてください。プロテクターイメージのダウンロードに関する詳細については、[こちら](#)を参照してください。SDXアプライアンスでManagement Serviceビルド118.7以降を使用していることを確認してください。

Configuration タブで、**Websense Protector > Software Images** に移動します。

XVAイメージをSDXアプライアンスにアップロードするには

1. 詳細ペインで、**XVA Files > Action** の下にある **Upload** をクリックします。
2. 表示されるダイアログボックスで、[こちら](#) をクリックし、アップロードするXVAファイルを選択します。
3. **Upload** をクリックします。XVAファイルがXVA Filesペインに表示されます。

Websense protectorインスタンスをプロビジョニングするには

1. **Configuration** タブで、**Websense Protector > Instances** に移動します。
2. 詳細ペインで、**Add** をクリックします。
3. **Provision Websense Protector** ウィザードで、画面の指示に従います。
4. **Finish** をクリックし、次に **Close** をクリックします。

インスタンスをプロビジョニングした後、そのインスタンスにログオンし、詳細な構成を実行します。

プロビジョニングされたWebsense protectorインスタンスの設定を変更するには、Websense Protector Instancesペインで、変更するインスタンスを選択し、**Modify** をクリックします。Modify Websense Protectorウィザードで、パラメータを設定します。Websenseインスタンスのプロビジョニング時に選択されたインターフェイスは変更しないでください。XVAファイルは、インスタンスを削除して新しいものをプロビジョニングした後にのみ変更できます。

テクニカルサポートに提出するためのtarアーカイブを生成できます。テクニカルサポートファイルの生成については、「[テクニカルサポート用Tarアーカイブの生成](#)」を参照してください。

Websense Protectorインスタンスを監視する

SDXアプライアンスは、**SDXTools** のバージョン、Websense Data Securityポリシーエンジンのステータス、およびData Securityプロキシのステータスなどの統計情報を収集します。

Websense protectorインスタンスに関連する統計情報を表示するには：

1. **Websense Protector > Instances** に移動します。

2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

Websense Protectorインスタンスを管理する

Management ServiceからWebsense protectorインスタンスを開始、停止、再起動、強制停止、または強制再起動できます。

「**Configuration**」タブで、「**Websense Protector**」を展開します。

Websense Protectorインスタンスを開始、停止、再起動、強制停止、または強制再起動するには

1. 「**Instances**」をクリックします。
2. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。
 - 開始
 - シャットダウン
 - 再起動
 - 強制シャットダウン
 - 強制再起動
3. 確認メッセージボックスで、「**Yes**」をクリックします。

Websense ProtectorインスタンスのSDXツールファイルをアップグレードする

サードパーティインスタンスで実行されているデーモンである **SDXTools** は、Management Serviceとサードパーティインスタンス間の通信に使用されます。

SDXTools のアップグレードには、ファイルをSDXアプライアンスにアップロードし、インスタンスを選択した後に **SDXTools** をアップグレードする作業が含まれます。クライアントコンピューターからSDXアプライアンスに **SDXTools** ファイルをアップロードできます。

SDXツールファイルをアップロードするには

1. ナビゲーションペインで、「**Management Service**」を展開し、「**SDXTools Files**」をクリックします。
2. 詳細ペインで、アクションリストから**アップロード**を選択します。

3. **SDXTools**ファイルのアップロードダイアログボックスで、**参照**をクリックし、ファイルが含まれるフォルダーに移動して、ファイルをダブルクリックします。
4. **アップロード**をクリックします。

SDXツールをアップグレードするには

構成タブで、**Websense Protector**を展開します。

1. **インスタンス**をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. アクションリストから**SDXTools**のアップグレードを選択します。
4. **SDXTools**のアップグレードダイアログボックスで、ファイルを選択し、**OK**をクリックしてから**閉じる**をクリックします。

Websense Protectorインスタンスを新しいバージョンにアップグレードする

Websense Protectorインスタンスをアップグレードするプロセスには、ターゲットビルドのソフトウェアイメージをSDXアプライアンスにアップロードし、その後インスタンスをアップグレードする作業が含まれます。

構成タブで、**Websense Protector**を展開します。

ソフトウェアイメージをアップロードするには

1. ソフトウェアイメージをクリックします。
2. 詳細ペインで、アクションリストから**アップロード**を選択します。
3. ダイアログボックスで、**Browse** をクリックし、ビルドファイルを含むフォルダーに移動して、ビルドファイルをダブルクリックします。
4. **Upload** をクリックします。

インスタンスをアップグレードするには

1. **Instances** をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. **Action** リストから、**Upgrade** を選択します。
4. 表示されるダイアログボックスで、ファイルを選択し、**OK** をクリックしてから、**Close** をクリックします。

Websense Protector インスタンスのトラブルシューティング

Management Service から Websense Protector インスタンスに ping を実行して、デバイスに到達可能かどうかを確認します。Management Service からインスタンスへのパケットのルートをトレースして、インスタンスに到達するまでにかかるホップ数を特定できます。

インスタンスを再検出して、インスタンスの最新の状態と構成を表示します。再検出中に、Management Service は、SDX アプライアンスで実行されている Websense Protector の構成とバージョンを取得します。デフォルトでは、Management Service は 30 分に 1 回、インスタンスの再検出をスケジュールします。

Configuration タブで、**Websense Protector** を展開します。

インスタンスに ping を実行するには

1. **Instances** をクリックします。
2. 詳細ペインで、ping を実行するインスタンスを選択し、**Action** リストから **Ping** をクリックします。Ping メッセージボックスに、ping が成功したかどうかが表示されます。

インスタンスのルートをトレースするには

1. 「**インスタンス**」をクリックします。
2. 詳細ペインで、ルートをトレースするインスタンスを選択し、「**アクション**」リストから「**TraceRoute**」をクリックします。Tracerouteメッセージボックスに、インスタンスへのルートが表示されます。

インスタンスを再検出するには

1. 「**インスタンス**」をクリックします。
2. 詳細ペインで、再検出するインスタンスを選択し、「**アクション**」リストから「**再検出**」をクリックします。
3. 確認メッセージボックスで、「**はい**」をクリックします。

BlueCat DNS/DHCP

BlueCat DNS/DHCPサーバーは、NetScaler SDXアプライアンスでサポートされているソフトウェアソリューションです。NetScaler SDXプラットフォーム上でホストされ、追加の管理コストやデータセンターのスペースを発生させることなく、信頼性が高く、スケーラブルで安全なDNSおよびDHCPコアネットワークサービスを提供します。重要なDNSサービスは、単一システム内の複

数のDNSノード間、または複数のSDXアプライアンス間で、追加のハードウェアを必要とせずにロードバランスできます。

BlueCat DNS/DHCPサーバーの仮想インスタンスは、SDX上でホストでき、モバイルデバイス、アプリケーション、仮想環境、クラウドを接続するためのよりスマートな方法を提供します。

BlueCatとCitrixの詳細については、BlueCatのウェブサイト (<https://citrixready.citrix.com/bluecat-networks.html>) をご覧ください。

既存のBlueCatのお客様は、BlueCatサポートポータル (<https://care.bluecatnetworks.com/>) からソフトウェアとドキュメントをダウンロードできます。

BlueCat DNS/DHCPインスタンスのプロビジョニング

BlueCatカスタマーケア (<https://care.bluecatnetworks.com>) からXVAイメージをダウンロードしてください。XVAイメージをダウンロードしたら、インスタンスのプロビジョニングを開始する前にSDXアプライアンスにアップロードしてください。SDXアプライアンスでManagement Serviceビルド118.7以降を使用していることを確認してください。

0/1および0/2インターフェイス間の管理チャネルは、BlueCat DNS/DHCP VMでサポートされています。詳細については、「[\(../configuring-management-service/configuring-channel-from-management-service.html\)](#)」を参照してください。

注: チャネルの一部であるSR-IOVインターフェイス (1/xおよび10/x) は、BlueCat DNS/DHCPインスタンスではチャネルがサポートされていないため、インターフェイスのリストには表示されません。

構成タブで、BlueCat DNS/DHCP > ソフトウェアイメージに移動します。

XVAイメージをSDXアプライアンスにアップロードするには:

1. 詳細ペインの**XVAファイル > アクション**で、**アップロード**をクリックします。
2. 表示されるダイアログボックスで、**参照**をクリックし、アップロードするXVAファイルを選択します。
3. **アップロード**をクリックします。XVAファイルがXVAファイルペインに表示されます。

BlueCat DNS/DHCPインスタンスをプロビジョニングするには:

1. 「Configuration」タブで、「BlueCat DNS/DHCP」 > 「Instances」に移動します。
2. 詳細ペインで、「Add」をクリックします。「Provision BlueCat DNS/DHCP Server」ページが開きます。

3. 「Provision BlueCat DNS/DHCP」ウィザードで、画面の指示に従います。

- 「Instance Creation」の下にある「Name」フィールドにインスタンスの名前を入力し、「XVA File」ドロップダウンメニューからアップロードされたイメージを選択して、「Next」をクリックします。オプションで、「Domain Name」フィールドにインスタンスのドメイン名を入力します。注: 名前にスペースを含めることはできません。
- 「Network Settings」の下にある「Management Interface」ドロップダウンメニューから、インスタンスを管理するインターフェイスを選択し、そのインターフェイスのIPアドレスとゲートウェイを設定します。高可用性とサービスのためにインターフェイスを明示的に割り当てることができます。パラメーターを選択し、「Next」をクリックします。

注: 管理、高可用性、およびサービスのためにインターフェイスを割り当ての際は、サポートされているインターフェイスの組み合わせに基づいてインターフェイスを割り当ててください。

3つすべてに同じインターフェイスを選択できます。3つすべてに異なるインターフェイスを選択できます。管理とサービスに同じインターフェイスを選択し、高可用性には異なるインターフェイスを選択できます。「Finish」をクリックし、次に「Close」をクリックします。インスタンスが作成され、起動し、選択したIPアドレスで構成されます。

インスタンスをプロビジョニングした後、SSH経由でインスタンスにログオンして構成を完了します。BlueCat DNS/DHCP Serverの構成、またはBlueCat Address Managerの制御下に置く方法の詳細については、<https://care.bluecatnetworks.com> で入手できるBlueCatのドキュメントを参照してください。

BlueCat DNS/DHCP Serverインスタンスの設定を変更するには、「BlueCat DNS/DHCP Instances」ペインから変更したいインスタンスを選択し、「Modify」をクリックします。

「Modify BlueCat DNS/DHCP」ウィザードで、パラメーター設定を変更します。

注: インターフェイスパラメーターまたはインスタンスの名前を変更すると、変更を有効にするためにインスタンスが停止して再起動します。

BlueCat DNS/DHCPインスタンスを監視する

SDXアプライアンスは、BlueCat DNS/DHCPインスタンスの、インスタンスで実行されているSDXTools のバージョンなどの統計情報を収集します。

BlueCat DNS/DHCPインスタンスに関連する統計情報を表示するには：

1. 「BlueCat DNS/DHCP」>「Instances」に移動します。
2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

BlueCat DNS/DHCPインスタンスの管理

Management ServiceからBlueCat DNS/DHCPインスタンスを開始、停止、再起動、強制停止、または強制再起動できます。

「**Configuration**」タブで、「**BlueCat DNS/DHCP**」を展開します。

BlueCat DNS/DHCPインスタンスを開始、停止、再起動、強制停止、または強制再起動するには:

1. 「**Instances**」をクリックします。
2. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。
 - 開始
 - シャットダウン
 - 再起動
 - 強制シャットダウン
 - 強制再起動
3. 確認メッセージボックスで、「**Yes**」をクリックします。

BlueCat DNS/DHCPインスタンスの **SDXTools** ファイルをアップグレードする

サードパーティインスタンスで実行されているデーモンである **SDXTools** は、Management Serviceとサードパーティインスタンス間の通信に使用されます。

SDXTools のアップグレードには、ファイルをSDXアプライアンスにアップロードし、インスタンスを選択した後に **SDXTools** をアップグレードする作業が含まれます。クライアントコンピュータからSDXアプライアンスに **SDXTools** ファイルをアップロードできます。

SDXToolsファイルをアップロードするには:

1. ナビゲーションペインで、**Management Service**を展開し、次に**SDXTools Files**をクリックします。
2. 詳細ペインで、**Action**リストから**Upload**を選択します。
3. **Upload SDXTools Files**ダイアログボックスで、**Browse**をクリックし、ファイルが含まれているフォルダーに移動し、次にファイルをダブルクリックします。
4. **Upload**をクリックします。

SDXToolsをアップグレードするには:

Configurationタブで、**BlueCat DNS/DHCP**を展開します。

1. **Instances**をクリックします。
2. 詳細ペインで、インスタンスを選択します。
3. Actionリストから、**Upgrade SDXTools**を選択します。
4. **Upgrade SDXTools**ダイアログボックスで、ファイルを選択し、**OK**をクリックし、次に**Close**をクリックします。

BlueCat DNS/DHCPインスタンスを再検出する

インスタンスを再検出して、インスタンスの最新の状態と構成を表示できます。再検出中に、Management Serviceは構成をフェッチします。デフォルトでは、Management Serviceはすべてのインスタンスの再検出を30分ごとに1回スケジュールします。

Configurationタブで、**BlueCat DNS/DHCP**を展開します。

1. **Instances**をクリックします。
2. 詳細ペインで、再検出したいインスタンスを選択し、**アクション**リストから**再検出**をクリックします。
3. **確認**メッセージボックスで、**はい**をクリックします。

CAアクセスゲートウェイ

CA Access Gatewayは、アクセス制御のためのプロキシベースのソリューションを提供する、スケーラブルで管理しやすく、拡張可能なスタンドアロンサーバーです。CA Access Gatewayは、企業向けにネットワークゲートウェイを提供するプロキシエンジンを採用しており、従来のクッキーベースのテクノロジーに依存しない複数のセッションスキームをサポートしています。

組み込みWebエージェントは、企業全体でのシングルサインオン (SSO) を可能にします。CA Access Gatewayは、HTTPおよびHTTPSリクエストのアクセス制御とクッキーレスSSOを提供します。また、この製品はセッション情報をインメモリセッションストアに保存します。プロキシルールは、CA Access Gatewayが企業内の宛先サーバー上にあるリソースへのリクエストをどのように転送またはリダイレクトするかを定義します。

ネットワークリソースに単一のゲートウェイを提供することで、CA Access Gatewayは企業ネットワークを分離し、アクセス制御を一元化します。

注: チャンネルの一部であるSR-IOVインターフェース (1/xおよび10/x) は、CA Access Gatewayインスタンスではチャンネルがサポートされていないため、インターフェースのリストには表示されませ

ん。CA Access Gatewayの機能の詳細については、その製品のドキュメントを参照してください。

CA Access Gatewayインスタンスのプロビジョニング

CA Access Gatewayインスタンスをプロビジョニングする前に、XVAイメージをダウンロードする必要があります。XVAイメージをダウンロードしたら、SDXアプライアンスにアップロードします。SDXアプライアンスでManagement Serviceバージョン10.5ビルド52.3.e以降を使用していることを確認してください。CA Access Gatewayをプロビジョニングするには、まずXVAイメージをSDXアプライアンスにアップロードし、その後インスタンスをプロビジョニングする必要があります。

XVAイメージをSDXアプライアンスにアップロードするには:

1. **Configuration**タブで、**CA Access Gateway > Software Images**に移動します。
2. 詳細ペインの**XVA Files**の下にある**Action**ドロップダウンリストから、**Upload**をクリックします。
3. 表示されるダイアログボックスで、**Browse**をクリックし、アップロードしたいXVAファイルを選択します。
4. **Upload**をクリックします。XVAファイルが**XVA Files**ペインに表示されます。

CA Access Gatewayインスタンスをプロビジョニングするには:

1. **Configuration**タブで、**CA Access Gateway > Instances**に移動します。
2. 詳細ペインで、**Add**をクリックします。
3. 「CA Access Gateway のプロビジョニング」ウィザードで、画面の指示に従います。
4. をクリックし、次に をクリックします。

インスタンスをプロビジョニングしたら、インスタンスにログオンして詳細な構成を実行します。

プロビジョニングされたインスタンスのパラメータの値を変更するには、詳細ペインで変更するインスタンスを選択し、 をクリックします。「CA Access Gateway の変更」ウィザードで、環境に適した値にパラメータを設定します。

注:

インターフェイスパラメータまたはインスタンスの名前を変更すると、変更を有効にするためにインスタンスが停止して再起動します。

CA Access Gateway インスタンスを監視する

SDXアプライアンスは、CA Access Gateway インスタンスについて、インスタンスで実行されている **SDXTools** のバージョンなどの統計情報を収集します。

CA Access Gateway インスタンスに関連する統計情報を表示するには:

1. > に移動します。
2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

CA Access Gateway インスタンスを管理する

Management Service から CA Access Gateway インスタンスを開始、停止、再起動、強制停止、または強制再起動できます。これらのタスクを完了するには、次の手順に従います。

1. タブで、 を展開します。
2. > に移動します。
3. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。
 - 起動
 - シャットダウン
 - 再起動
 - 強制シャットダウン
 - 強制再起動
4. 確認メッセージボックスで、「はい」をクリックします。

パロアルトネットワークス VMシリーズ

Palo Alto Networks VM-Series仮想ファイアウォールは、同社の物理セキュリティアプライアンスで利用可能なものと同じPAN-OS機能セットを使用し、すべての主要なネットワークセキュリティ機能を提供します。NetScaler SDX上のVM-Seriesは、高度なセキュリティ機能とADC機能を単一プラットフォームに統合することを可能にし、企業、事業部門、サービスプロバイダーの顧客によるアプリケーションへの安全で信頼性の高いアクセスを実現します。NetScaler SDX上のVM-Seriesの組み合わせは、Citrix Virtual Apps and Desktopsの展開向けに、完全で検証済みのセキュリティおよびADCソリューションも提供します。

Management Serviceからインスタンスのプロビジョニング、監視、管理、トラブルシューティングを行うことができます。

注意点：

- SDXアプライアンスでプロビジョニングできるインスタンスの総数は、利用可能なSDXハードウェアリソースによって異なります。
- チャンネルの一部であるSR-IOVインターフェイス (1/xおよび10/x) は、Palo Alto VM-Seriesインスタンスではチャンネルがサポートされていないため、インターフェイスのリストに表示されません。Palo Alto Network VM-Seriesの詳細については、[Palo Alto Network Documentation](#)を参照してください。

Palo Alto VM-Seriesインスタンスのプロビジョニング

Palo Alto VM-Seriesインスタンスをプロビジョニングする前に、[Palo Alto Networks website](#)からXVAイメージをダウンロードする必要があります。XVAイメージをダウンロードしたら、SDXアプライアンスにアップロードします。

XVAイメージをSDXアプライアンスにアップロードするには：

1. **Configuration**タブで、**PaloAlto VM-Series > Software Images**に移動します。
2. 詳細ペインの**XVA Files**の下にある**Action**ドロップダウンリストから、**Upload**をクリックします。
3. 表示されるダイアログボックスで**Browse**をクリックし、アップロードするXVAファイルを選択します。
4. **Upload**をクリックします。XVAファイルが**XVA Files**ペインに表示されます。

Palo Alto VM-Seriesインスタンスをプロビジョニングするには：

1. **Configuration**タブで、**PaloAlto VM-Series > Instances**に移動します。
2. 詳細ペインで、**追加**をクリックします。
3. PaloAlto VM-Seriesプロビジョニングウィザードで、画面の指示に従います。
4. **完了**をクリックし、次に**閉じる**をクリックします。

インスタンスをプロビジョニングした後、インスタンスにログオンし、詳細な構成を実行します。

プロビジョニングされたインスタンスのパラメータの値を変更するには、詳細ペインで変更するインスタンスを選択し、**変更**をクリックします。PaloAlto VM-Series変更ウィザードで、環境に適した値にパラメータを設定します。

注: インターフェイスパラメータまたはインスタンスの名前を変更すると、変更を有効にするためにインスタンスが停止して再起動します。

Palo Alto VM-Seriesインスタンスを監視する

SDXアプライアンスは、Palo Alto VM-Seriesインスタンスで実行されている **SDXTools** のバージョンなどの統計情報を収集します。

Palo Alto VM-Seriesインスタンスに関連する統計情報を表示するには：

1. **PaloAlto VM-Series > インスタンス**に移動します。
2. 詳細ペインで、インスタンス名の横にある矢印をクリックします。

PaloAlto VM-Seriesインスタンスを管理する

Management ServiceからPaloAlto VM-Seriesインスタンスを開始、停止、再起動、強制停止、または強制再起動できます。

構成タブで、**PaloAlto VM-Series**を展開します。

1. **PaloAlto VM-Series > インスタンス**に移動します。
2. 詳細ペインで、操作を実行するインスタンスを選択し、次のいずれかのオプションを選択します。
 - 開始
 - シャットダウン
 - 再起動
 - 強制シャットダウン
 - 強制再起動
3. 確認メッセージボックスで、「はい」をクリックします。

PaloAlto VM-Seriesインスタンスのトラブルシューティング

Management ServiceからPaloAlto VM-SeriesインスタンスをPingして、デバイスに到達可能かどうかを確認します。Management Serviceからインスタンスへのパケットのルートをトレースして、インスタンスに到達するまでのホップ数を特定できます。

インスタンスを再検出して、インスタンスの最新の状態と構成を表示します。再検出中に、Management ServiceはSDXアプライアンスで実行されているPaloAlto VM-Seriesの構成とバージョンを取得します。デフォルトでは、Management Serviceは30分ごとにインスタンスの再検出をスケジュールします。

「**構成**」タブで、「**PaloAlto VM-Series**」を展開します。

インスタンスをPingするには：

1. 「**インスタンス**」をクリックします。
2. 詳細ペインで、Pingするインスタンスを選択し、「**アクション**」リストから「**Ping**」をクリックします。「**Pingメッセージ**」ボックスにPingが成功したかどうかが表示されます。

インスタンスのルートをトレースするには：

1. 「**インスタンス**」をクリックします。
2. 詳細ペインで、pingを実行したいインスタンスを選択し、「**アクション**」リストから「**TraceRoute**」をクリックします。「**Traceroute**」メッセージボックスに、そのインスタンスへのルートが表示されます。

インスタンスを再検出するには：

1. 「**インスタンス**」をクリックします。
2. 詳細ペインで、再検出したいインスタンスを選択し、「**アクション**」リストから「**Rediscover**」をクリックします。
3. 確認メッセージボックスで、「**はい**」をクリックします。

NetScaler SDXアプライアンスにCitrix SD-WAN VPXインスタンスを展開する

Citrix SD-WANテクノロジーは、ソフトウェア定義ネットワーク (SDN) の概念をWAN接続に適用します。このテクノロジーは、トラフィック管理と監視をネットワークハードウェアから抽象化し、個々のアプリケーションに適用します。その結果、パフォーマンスが向上し、地理的に分散した場所での高品質なユーザーエクスペリエンスが実現され、広域ネットワークとクラウドアクセスネットワークの展開が簡素化されます。詳細については、[Citrix SD-WAN](#)を参照してください。

注: SD-WAN VPX Standardエディションのみがサポートされています。詳細については、[SD-WAN VPXエディション](#)を参照してください。

SDXアプライアンスにCitrix SD-WAN™ VPXインスタンスを展開するには、次のタスクが含まれます。

- ハードウェアのインストール: SDXハードウェアが適切にインストールされていることを確認します。詳細については、[ハードウェアのインストール](#)を参照してください。
- SDX Management Serviceのセットアップと構成。詳細については、[Management Serviceユーザーインターフェイスの概要](#)および[Management Serviceの構成](#)を参照してください。
- SDXアプライアンスへのSD-WAN VPXインスタンスのプロビジョニング。詳細については、[NetScaler SDXへのCitrix SD-WAN VPXインスタンスのプロビジョニング](#)を参照してください。
- SD-WAN VPXインスタンスの構成。詳細については、[構成ドキュメント](#)および[MCNとクライアントサイト間の仮想パスサービスの構成](#)を参照してください。

前提条件

次のライセンスがあることを確認してください。

- Citrix SD-WAN VPXライセンス
- NetScaler SDXプラットフォームライセンス

Citrix SD-WAN VPXの要件

SDXプラットフォーム上のCitrix SD-WAN VPXは、サイトとしてもMCNとしても機能できます。MCNは、1 Gb/sの双方向スループットと64サイトを処理できます。

MCNおよびサイトでサポートされるスループット

- 250 Mb/s から 1 Gb/s の双方向スループット
- MCN は 64 サイトに対応しています

サポートされるスループットのハードウェア要件

サイト

- 4 CPU から 16 CPU
- 4 GB から 16 GB RAM
- 60 GB から 250 GB ディスクストレージ
- 最小 4 つの NIC: 1 つは管理用、残りの最小 3 つはデータパス用

マスターコントロールノード (MCN)

- 4、8、および 16 CPU
- 16 GB RAM
- 250 GB ディスクストレージ
- 最小 4 つの NIC: 1 つは管理用、残りの 3 つはデータパス用、データパス専用の NIC を使用

データセンターのトポロジ

NetScaler SDX には、ポリシーベースルート (PBR) モードまたはインラインモードで Citrix SD-WAN VPX アプライアンスを展開できます。これら 2 つのサポートされるモードのデータセンターのトポロジについては、シナリオ 1 および 2 を参照してください。詳細については、[仮想インラインモードでの SD-WAN の展開](#) を参照してください。

シナリオ 1: インラインモード



シナリオ 2: PBRモードまたは仮想インラインモード



NetScaler SDX™ 上でのCitrix SD-WAN VPXインスタンスのプロビジョニング

Citrix SD-WAN VPXアプライアンスをプロビジョニングする前に、NetScaler®製品ダウンロードサイトからSD-WAN VPXイメージをダウンロードします。 [<https://www.citrix.com/downloads/netscaler-sd-wan/>](https://www.citrix.com/downloads/netscaler-sd-wan/)。

以下の手順に従って、Citrix SD-WAN VPXアプライアンスをプロビジョニングします。

1. NetScaler SDXアプライアンスにログオンします。
2. **Configuration > SD-WAN > Instances**に移動します。
3. **Software Images > Upload**を選択し、SD-WAN XVAファイルをアップロードします。



4. **Instances > Add**を選択します。 **Provision SD-WAN Instance**ページが表示されます。
5. **Provision SD-WAN Instance**ページで、以下を入力します。

- a. 名前
- b. IPアドレス
- c. ネットマスク
- d. ゲートウェイアドレス
- e. XVAファイルをアップロードする
- f. リソース割り当てで、リソースを割り当てます。



- g. **ネットワーク設定**で、管理インターフェイスをプロビジョニングし、**OK**を選択してSDXアプライアンスにSD-WAN VPXインスタンスをプロビジョニングします。

注：

SDX管理サービスは、インターフェイス名を昇順にVPXインスタンスにバインドします。たとえば、1/4と1/1を追加すると、管理サービスはそれらを1/1、1/4として配置します。新しいインターフェイスを追加すると、既存のシーケンスが保持され、新しいシーケンスが作成されます。たとえば、インターフェイス1/2、10/1、1/3を追加すると、新しいシーケンスは1/1、1/4; 1/2、1/3、10/1になります。

6. SD-WAN VPXインスタンスは、**インスタンスページ**に表示されます。以下に例を示します。

! [Image] (<https://docs.netscaler.com/content/dam/netscaler/us/en/sdx/media/sd-wan-vpx-example.png>)

インスタンスを編集するには、**構成 > SD-WAN > インスタンス**に移動します。インスタンスを選択してクリックします。編集が完了したら、**OK**をクリックして変更を保存します。

Citrix SD-WAN VPXインスタンスの構成

SDXアプライアンスにSD-WANインスタンスを作成したら、次の2つのタスクを完了してSD-WANインスタンスを構成します。

1. MCNアプライアンスとサイトアプライアンスの両方に構成を適用します。
2. 仮想パスを構成し、トラフィックを送信します。

詳細については、次のトピックを参照してください。

- [構成](#)
- [MCNとクライアントサイト間の仮想パスサービスの設定](#)

関連情報

Citrix SD-WANアプライアンスの使用開始について詳しくは、[Citrix SD-WAN](#)を参照してください。

NetScaler SDXアプライアンスについて詳しくは、[NetScaler SDX](#)を参照してください。

SDXにおける帯域幅メータリング

NetScaler SDXの帯域幅メータリングは、正確で信頼性が高く、使いやすいメータリングスキームを提供し、処理能力を効率的に割り当て、帯域幅の使用状況を収益化できます。すべてのユーザーが常に割り当てられた帯域幅を得られるように、さまざまなリソース間で帯域幅を最適に割り当てるには、メータリングスキームが必要です。

帯域幅の割り当ては、次の2つのモードで行うことができます。

- 固定スループットレートの専用帯域幅
- 最小保証スループットと帯域幅バースト機能を備えた専用帯域幅

固定スループットレートの専用帯域幅

この帯域幅割り当て方法では、各VPXインスタンスに専用の帯域幅が割り当てられます。インスタンスは、設定された制限まで帯域幅を使用できます。専用モードでは、割り当てられる最小帯域幅と最大帯域幅は同じです。ある期間中にVPXインスタンスが割り当てられた帯域幅よりも多くの帯域幅を必要とする場合、専用モードではインスタンスはそのスループットを増やすことができません。VPXインスタンスが重要なリクエストを処理する場合、この問題は欠点となる可能性があります。

また、SDXアプライアンスにいくつかのVPXインスタンスがあり、その一部が割り当てられた帯域幅を利用していない場合、専用モードではその未使用の帯域幅を共有することはできません。これらの課題をすべて克服するには、最小保証レートで帯域幅を動的に増加させる機能を備えた専用帯域幅が役立ちます。

最小保証スループットと帯域幅バースト機能を備えた専用帯域幅

この帯域幅割り当て方法では、VPXには最小保証帯域幅が割り当てられ、事前に設定された制限まで帯域幅を増やす柔軟性があります。VPXが使用できる追加の帯域幅は、バースト容量と呼ばれます。

バースト容量の利点は、余分な容量を持つインスタンスと、未使用の容量を持つVPXがある場合に現れます。これらのVPXインスタンスの余分な容量は、割り当てられた帯域幅を完全に使い果たし、一時的にさらに多くの帯域幅を必要とする他のVPXインスタンスに割り当てることができます。さまざまなサービスプロバイダーも、専用容量を必要とする顧客にさまざまなアドオンサー

ビスを提供することに関心があります。同時に、帯域幅を過剰にプロビジョニングしたくありません。バースト可能な帯域幅は、顧客が特定の帯域幅を保証され、需要が高い期間中に帯域幅を増やすオプションがあるようなシナリオで役立ちます。

帯域幅割り当てモードの選択

バースト可能なスループットを選択する前に、動的バーストスループット割り当てを有効にする必要があります。このオプションを有効にするには、次の手順に従います。

1. SDX管理コンソールから、**Configuration > System**に移動します。
2. **System Settings**グループから、**Change System Settings**を選択します。
3. 「動的バーストスループット割り当てを有効にする」チェックボックスをクリックして、動的スループットを有効にします。



VPXをプロビジョニングする際、帯域幅バーストまたは動的スループットを選択できます。

1. **SDX Management Service**で、**Configuration > NetScaler > Instances > Add**をクリックします。
2. **NetScaler**のプロビジョニングページが開きます。「ライセンス割り当て」で、「割り当てモード」から「バースト可能」を選択します。



NetScalerインスタンスのプロビジョニング方法の詳細については、「[NetScalerインスタンスのプロビジョニング](#)」を参照してください。

固定スループットを使用する場合は、「**固定**」を選択します。デフォルトでは、帯域幅割り当てには固定モードが設定されています。すべてのVPXインスタンスが同じモードで動作する必要はありません。各VPXインスタンスは異なるモードで構成できます。

注: SDXを10.5.e以前のバージョンから移行する場合、デフォルトではすべてのVPXインスタンスが固定割り当てモードになります。

VPXインスタンスの最大バースト帯域幅の決定

各VPXがバーストを許可される範囲は、アルゴリズムによって計算されます。バースト可能な帯域幅を持つVPXをプロビジョニングする場合、そのような各VPXには優先順位を付与する必要があります。バースト可能な帯域幅の割り当ては、このバースト優先順位に依存します。優先順位はP0からP4まであり、P0が最も高く、P4が最も低くなります。

VPX1とVPX2という2つのVPXがあるケースを考えてみましょう。VPX1とVPX2に割り当てられる最小帯域幅はそれぞれ4 Gbpsと2 Gbpsで、バースト可能な帯域幅はそれぞれ2 Gbpsと1 Gbpsです。次の表にパラメータを示します。

VPX名	パラメータ	値	
VPX1	最小保証帯域幅	4ギガビット/秒	
-	-	最大バースト可能帯域幅	2ギガビット/秒
-	-	優先度	P0
VPX2	最小保証帯域幅	2ギガビット/秒	
-	-	最大バースト可能帯域幅	1ギガビット/秒
-	-	優先度	P1

このケースでは、合計ライセンス帯域幅が8 Gbpsであると仮定します。両方のVPXインスタンスが最大バースト可能制限までバーストしている場合、つまり次のようになります。

1. VPX1がその最大バースト可能帯域幅、つまり2 Gbpsを使用している場合、合計で $4 + 2 = 6$ Gbpsを使用しています。
2. VPX2がその最大バースト可能帯域幅、つまり1 Gbpsを使用している場合、合計で $2 + 1 = 3$ Gbpsを使用しています。

この場合、使用される最大帯域幅は、ライセンス容量の8 Gbpsを超えています。そのため、使用量をライセンス容量内の帯域幅に抑えるには、いずれかのVPXがバースト可能帯域幅を放棄する必要があります。このケースでは、VPX2がVPX1よりも優先度が低いため、1 Gbpsのバースト可能帯域幅を放棄します。VPX1はVPX2よりも優先度が高いため、バーストを継続します。このようなすべてのシナリオにおいて、最小保証帯域幅は常に尊重されるようにします。

スループットとデータ消費統計の確認

各VPXについて、グラフでスループットとデータ消費統計を確認できます。グラフにアクセスするには、次の手順に従います。

1. SDX管理サービスから、**構成 > NetScaler > インスタンス** ページに移動します。
2. VPXインスタンスを選択し、**アクション** ドロップダウンリストをクリックします。

3. リストから、スループット統計またはデータ使用量統計のいずれかを選択します。

グラフでは、データ消費量とスループット統計をさまざまな期間について確認できます。例えば：

- 過去1時間
- 過去1日
- 過去1週間
- 過去1か月、および
- 前月

グラフの下部にあるスライダーを調整することで、グラフ内で特定の期間を選択することもできます。グラフの線にマウスを移動すると、特定の時間のデータ消費量またはスループットデータを確認できます。

次の図は、1週間のスループットデータのサンプルグラフを示しています：

スループットデータ(/en-us/sdx/media/metering_graph_slider-citrix.png)

NetScalerインスタンスの構成と管理

アプライアンスにNetScalerインスタンスをプロビジョニングした後、インスタンスを構成および管理する準備が整います。まず、サブネットIP（SNIP）アドレスを作成し、構成を保存します。その後、インスタンスで基本的な管理タスクを実行できます。管理構成を適用する必要があるかどうかを確認してください。

警告: インスタンスのプロビジョニングされたネットワークインターフェイスまたはVLANを変更する場合は、インスタンスで直接変更を行うのではなく、Management Serviceを使用してください。

NetScalerインスタンスでSNIPアドレスを作成する

SDXアプライアンスにプロビジョニングされた後、NetScalerインスタンスにSNIPアドレスを割り当てることができます。

SNIPは、接続管理とサーバー監視に使用されます。NetScaler SDXアプライアンスを最初に構成するときにSNIPを指定することは必須ではありません。Management ServiceからNetScalerインスタンスにSNIPを割り当てることができます。

NetScalerインスタンスにSNIPアドレスを追加するには

1. **構成**タブのナビゲーションペインで、**NetScaler**をクリックします。
2. 詳細ペインの**NetScaler構成**の下にある**IPの作成**をクリックします。
3. **NetScaler IPの作成**ダイアログボックスで、次のパラメーターの値を指定します。
 - **IPアドレス:** SNIPアドレスとして割り当てられたIPアドレスを指定します。
 - **ネットマスク:** SNIPアドレスに関連付けられたサブネットマスクを指定します。
 - **タイプ:** デフォルト値はSNIPです。
 - **構成の保存:** NetScalerに構成を保存するには、これを選択します。デフォルト値はfalseです。
 - **インスタンスIPアドレス:** NetScalerインスタンスのIPアドレスを指定します。
4. 「作成」をクリックし、「閉じる」をクリックします。

構成を保存する

Management ServiceからNetScalerインスタンスの 実行中の構成を保存できます。

NetScalerインスタンスの構成を保存するには

1. 「**構成**」タブのナビゲーションペインで、「**NetScaler**」をクリックします。
2. 詳細ペインの「**NetScaler構成**」で、「**構成の保存**」をクリックします。
3. 「**構成の保存**」ダイアログボックスの「**インスタンスIPアドレス**」で、構成を保存する NetScalerインスタンスのIPアドレスを選択します。
4. 「**OK**」をクリックし、「**閉じる**」をクリックします。

NetScalerインスタンスを管理する

Management Serviceでは、NetScalerインスタンスに対して次の操作を実行できます。「**構成**」タブの「**NetScalerインスタンス**」ペイン、またはホームページのNetScalerインスタンスガジェットからこれらの操作を実行できます。

NetScalerインスタンスの起動: Management Serviceユーザーインターフェイスから任意の NetScalerインスタンスを起動します。Management Service UIがこの要求をManagement Serviceに転送すると、NetScalerインスタンスが起動します。

NetScalerインスタンスのシャットダウン: Management Serviceユーザーインターフェイスから任意のNetScalerインスタンスをシャットダウンします。Management Service UIがこの要求をManagement Serviceに転送すると、NetScalerインスタンスが停止します。

NetScalerインスタンスの再起動: NetScalerインスタンスを再起動します。

NetScalerインスタンスの削除: NetScalerインスタンスを使用しない場合は、Management Serviceを使用してそのインスタンスを削除できます。インスタンスを削除すると、そのインスタンスと関連する詳細が SDXアプライアンスのデータベースから完全に削除されます。

NetScalerインスタンスを起動、停止、削除、または再起動するには

1. 「**Configuration**」タブのナビゲーションペインで、「**NetScaler instances**」をクリックします。
2. 操作を実行するNetScalerインスタンスを選択し、「**Start**」または「**Shut Down**」または「**Delete**」または「**Reboot**」をクリックします。
3. 確認メッセージボックスで、「**Yes**」をクリックします。

NetScalerインスタンスファイルの削除

アプライアンスから、XVA、ビルド、ドキュメント、SSLキー、SSL証明書などのNetScalerインスタンスファイルを削除できます。

NetScalerインスタンスファイルを削除するには

1. 「**Configuration**」タブのナビゲーションペインで、「**NetScaler Configuration**」を展開し、削除するファイルをクリックします。
2. 詳細ペインでファイル名を選択し、「**Delete**」をクリックします。

管理構成を適用する

VPXインスタンスのプロビジョニング時に、Management ServiceはVPXインスタンス上にいくつかのポリシー、インスタンス管理（admin）プロファイル、およびその他の構成を作成します。Management Serviceが管理構成の適用に失敗した場合、Management ServiceからVPXインスタンスに構成を明示的にプッシュできます。失敗の理由の1つは、Management ServiceとVPXインスタンスが異なるサブネットワーク上にあり、ルーターがダウンしていることかもしれません。もう1つの理由は、両方が同じサブネット上にあるが、トラフィックが外部スイッチを通過する必要があり、リンクの1つがダウンしていることかもしれません。

NetScalerインスタンスに管理構成を適用するには

1. 「**Configuration**」タブのナビゲーションペインで、「**NetScaler**」をクリックします。
2. 詳細ペインの「**NetScaler Configuration**」の下にある「**Apply Admin Configuration**」をクリックします。
3. 「**Apply Admin Configuration**」ダイアログボックスの「**Instance IP Address**」で、管理構成を適用するVPXインスタンスのIPアドレスを選択します。
4. 「**OK**」をクリックします。

SSL証明書のインストールと管理

SSL証明書のインストールプロセスには、まず証明書とキーファイルをNetScaler SDXアプライアンスにアップロードすることが含まれます。次に、NetScalerインスタンスにSSL証明書をインストールします。SDXアプライアンスにSSL証明書をインストールまたは更新すると、管理サービスが再起動します。

証明書ファイルをSDXアプライアンスにアップロードする

すべてのSSLトランザクションには、サーバーは有効な証明書と、対応する秘密鍵および公開鍵のペアを必要とします。NetScalerインスタンスにSSL証明書をインストールする際には、証明書ファイルがSDXアプライアンスに存在している必要があります。SSL証明書ファイルをバックアップとしてローカルコンピューターにダウンロードすることもできます。

SSL証明書ペインで、次の詳細を表示できます。

- **名前**

証明書ファイルの名前。

- **最終更新日時**

証明書ファイルが最後に変更された日付。

- **サイズ**

証明書ファイルのサイズ（バイト単位）。

SSL証明書ファイルをSDXアプライアンスにアップロードするには

1. ナビゲーションペインで、を展開し、をクリックします。
2. ペインで、をクリックします。
3. ダイアログボックスで、をクリックし、アップロードする証明書ファイルを選択します。
4. 「アップロード」をクリックします。証明書ファイルがSSL証明書ペインに表示されます。

SSL証明書ファイルをダウンロードしてバックアップを作成するには

1. SSL証明書ペインで、ダウンロードするファイルを選択し、「ダウンロード」をクリックします。
2. メッセージボックスで、「保存」リストから「名前を付けて保存」を選択します。
3. 「名前を付けて保存」メッセージボックスで、ファイルを保存する場所を参照し、「保存」をクリックします。

SSLキーファイルをSDXアプライアンスにアップロードする

SSLトランザクションの場合、サーバーには有効な証明書と、対応する秘密鍵および公開鍵のペアが必要です。NetScalerインスタンスにSSL証明書をインストールする際には、キーファイルがSDXアプライアンスに存在している必要があります。バックアップとして、SSLキーファイルをローカルコンピューターにダウンロードすることもできます。

SSLキーペインでは、次の詳細を表示できます。

- **名前**

キーファイルの名前。

- **最終変更日時**

キーファイルが最後に変更された日付。

- **サイズ**

キーファイルのサイズ（バイト単位）。

SSLキーファイルをSDXアプライアンスにアップロードするには

1. ナビゲーションペインで、[キーファイル](#)を展開し、[アップロード](#)をクリックします。
2. ペインの [アップロード](#) タブで、[アップロード](#)をクリックします。
3. ダイアログボックスで、[アップロード](#)をクリックし、アップロードするキーファイルを選択します。
4. [アップロード](#)をクリックして、キーファイルを SDX アプライアンスにアップロードします。キーファイルはペインに表示されます。

SSLキーファイルをダウンロードしてバックアップを作成するには

1. ペインの [アップロード](#) タブで、ダウンロードするファイルを選択し、[ダウンロード](#)をクリックします。
2. メッセージボックスで、[ダウンロード](#) リストから [ダウンロード](#)を選択します。
3. メッセージボックスで、ファイルを保存する場所を参照し、[ダウンロード](#)をクリックします。

NetScalerインスタンスへのSSL証明書のインストール

Management Service を使用すると、1つ以上のNetScaler インスタンスにSSL証明書をインストールできます。SSL証明書のインストールを開始する前に、SSL証明書とキーファイルをSDXアプライアンスにアップロードしていることを確認してください。

NetScalerインスタンスにSSL証明書をインストールするには

1. ナビゲーションペインで、[証明書](#)をクリックします。
2. 詳細ペインの [証明書](#) で、[証明書](#)をクリックします。
3. ダイアログボックスで、次のパラメーターの値を指定します。（*）は必須フィールドを示します。

- 証明書ファイル: 有効な証明書のファイル名を指定します。証明書ファイルはSDXアプライアンスに存在する必要があります。
- キーファイル: 証明書の作成に使用された秘密鍵のファイル名を指定します。キーファイルはSDXアプライアンスに存在している必要があります。
- 証明書名: NetScalerに追加する証明書とキーのペアの名前を指定します。最大長: 31
- 証明書形式: NetScalerでサポートされているSSL証明書の形式を指定します。NetScaler SDXアプライアンスは、SSL証明書としてPEMおよびDER形式をサポートしています。
- パスワード: 秘密鍵の暗号化に使用されたパスフレーズを指定します。このオプションは、暗号化された秘密鍵をロードするために使用できます。最大長: 32。

注: パスワードで保護された秘密鍵は、PEM形式でのみサポートされます。

- 設定の保存: 設定をNetScalerに保存する必要があるかどうかを指定します。デフォルト値はfalseです。
- インスタンスIPアドレス: SSL証明書をインストールするNetScalerインスタンスのIPアドレスを指定します。

4. をクリックし、次にをクリックします。

NetScalerインスタンスでのSSL証明書の更新

NetScalerインスタンスにインストールされているSSL証明書の証明書ファイル、キーファイル、証明書形式などの一部のパラメータを更新できます。IPアドレスと証明書名は変更できません。

NetScalerインスタンスでSSL証明書を更新するには

1. ナビゲーションペインでを展開し、をクリックします。
2. ペインで、をクリックします。
3. ダイアログボックスで、次のパラメータを設定します。
 - 証明書ファイル: 有効な証明書のファイル名。証明書ファイルはSDXアプライアンスに存在している必要があります。
 - キーファイル: 証明書の作成に使用された秘密鍵のファイル名。キーファイルはSDXアプライアンス上に存在する必要があります。
 - 証明書形式: NetScaler SDXアプライアンスでサポートされているSSL証明書の形式。アプライアンスはSSL証明書にPEMおよびDER形式をサポートしています。
 - パスワード: 秘密鍵の暗号化に使用されたパスフレーズ。このオプションは、暗号化された秘密鍵をロードするために使用できます。最大長: 32文字。

注: パスワードで保護された秘密鍵はPEM形式でのみサポートされます。

- 設定の保存: 設定をSDXアプライアンスに保存する必要があるかどうかを指定します。デフォルト値はfalseです。
- ドメインチェックなし: 証明書の更新中にドメイン名をチェックしません。

4. OKをクリックし、その後閉じるをクリックします。

NetScalerインスタンスでのSSL証明書のポーリング

NetScalerインスタンスにログインした後、そのインスタンスに直接SSL証明書を追加した場合、Management Serviceはこの新しい証明書を認識しません。このシナリオを回避するには、Management ServiceがすべてのNetScalerインスタンスをポーリングして新しいSSL証明書をチェックするポーリング間隔を指定します。Management Serviceからいつでもポーリングを実行することもできます。たとえば、すべてのNetScalerインスタンスからSSL証明書のリストをすぐに取得したい場合などです。

ポーリング間隔を構成するには

1. ナビゲーションペインで、NetScalerを展開し、その後SSL証明書をクリックします。
2. SSL証明書ペインで、ポーリング間隔の構成をクリックします。
3. ポーリング間隔の構成ダイアログボックスで、次のパラメータを設定します。
 - ポーリング間隔: Management ServiceがNetScalerインスタンスをポーリングするまでの時間。
 - 間隔単位: 時間の単位。指定可能な値: 時間、分。デフォルト: 時間。
4. 「OK」をクリックし、次に「閉じる」をクリックします。

即時ポーリングを実行するには

1. ナビゲーションペインでNetScalerを展開し、次に「SSL Certificates」をクリックします。
2. 「SSL Certificates」ペインで、「今すぐポーリング」をクリックします。
3. 確認ダイアログボックスで「はい」をクリックします。「SSL Certificates」ペインが更新され、新しい証明書があればリストに表示されます。

NetScalerインスタンスでL2モードを許可する

レイヤー2 (L2) モードでは、NetScalerインスタンスは学習ブリッジとして機能し、自身が宛先ではないすべてのパケットを転送します。Citrix CloudBridgeなどの一部の機能では、NetScalerインスタンスでL2モードを有効にする必要があります。L2モードが有効になっている場合、インスタ

ンスは自身のMACアドレス以外のMACアドレス宛てのパケットを受信および転送できます。ただし、NetScaler SDXアプライアンスで実行されているNetScalerインスタンスでL2モードを有効にするには、管理者はまずそのインスタンスでL2モードを許可する必要があります。L2モードを許可する場合は、ブリッジンググループを回避するための予防措置を講じる必要があります。

注意事項:

1. 特定の1/xインターフェイスでは、タグなしパケットは1つのインスタンスでのみ許可する必要があります。同じインターフェイスで有効になっている他のすべてのインスタンスについては、「タグ付き」を選択する必要があります。

注:

Citrix®は、L2モードのインスタンスに割り当てられているすべてのインターフェイスで「タグ付き」を選択することを推奨します。タグ付きを選択した場合、そのインターフェイスでタグなしパケットを受信することはできません。

インスタンスに割り当てられているインターフェイスで「タグ付き」を選択した場合は、そのインスタンスにログオンし、そのインターフェイスでパケットを受信するように802.1q VLANを構成します。

2. L2モードが許可されているNetScalerインスタンスによって共有される1/xおよび10/xインターフェイスについては、次の条件が満たされていることを確認してください。
 - すべてのインターフェイスでVLANフィルタリングが有効になっていること。
 - 各インターフェイスが異なる802.1q VLAN上にあること。
 - インターフェイスでタグなしパケットを受信できるのは1つのインスタンスのみです。そのインターフェイスが他のインスタンスに割り当てられている場合は、それらのインスタンスに対してそのインターフェイスで「タグ付き」を選択する必要があります。
3. L2モードが許可されているインスタンスの1/xインターフェイスでタグなしパケットを許可する場合、他のインスタンスはそのインターフェイスでタグなしパケットを受信できません。この条件は、他のインスタンスでL2モードが許可されているか禁止されているかに関係なく適用されます。
4. L2モードが無効になっているインスタンスの1/xインターフェイスでタグなしパケットを許可する場合、L2モードが許可されているインスタンスはそのインターフェイスでタグなしパケットを受信できません。
5. L2モードでプロビジョニングされたinstance1に0/xインターフェイスが割り当てられており、そのインターフェイスがinstance2にも割り当てられている場合、instance2に割り当てられている他のすべてのインターフェイスで「タグ付き」を選択します。

注: 両方の管理インターフェイスがL2モードのインスタンスに割り当てられている場合、これらのインターフェイスのうち1つのみを、L2モードが有効になっている別のADCインスタンスに割り当てることができます。つまり、L2モードが有効になっている複数のNetScalerインスタンスに両方の管理インターフェイスを関連付けることはできません。

インスタンスでL2モードを許可するには

1. ADCプロビジョニングウィザードまたはADC変更ウィザードで、「**ネットワーク設定**」ページで「**L2モードを許可**」を選択します。 **注:** インスタンスをプロビジョニングするとき、またはインスタンスの実行中に、インスタンスでL2モードを許可する設定をアクティブにできません。
2. ウィザードの指示に従います。
3. 「完了」をクリックし、次に「閉じる」をクリックします。

インターフェースでの仮想MACの構成

NetScalerインスタンスは、高可用性（アクティブ-アクティブまたはアクティブ-スタンバイ）構成に仮想MAC（VMAC）を使用します。仮想MACアドレス（VMAC）は、高可用性セットアップにおいてプライマリノードとセカンダリノードで共有されるフローティングエンティティです。

高可用性セットアップでは、プライマリノードがMIP、SNIP、VIPアドレスなどのすべてのフローティングIPアドレスを所有します。プライマリノードは、これらのIPアドレスに対するアドレス解決プロトコル（ARP）要求に自身のMACアドレスで応答します。その結果、外部デバイス（例えば、アップストリームルーター）のARPテーブルは、フローティングIPアドレスとプライマリノードのMACアドレスで更新されます。

フェイルオーバーが発生すると、セカンダリノードが新しいプライマリノードとして引き継ぎます。その後、Gratuitous ARP（GARP）を使用して、プライマリから取得したフローティングIPアドレスをアドバタイズします。ただし、新しいプライマリがアドバタイズするMACアドレスは、自身のインターフェースのMACアドレスです。

一部のデバイス（特に一部のルーター）は、NetScaler SDXアプライアンスによって生成されたGARPメッセージを受け入れません。このようなデバイスは、古いプライマリノードによってアドバタイズされた古いIP-MACマッピングを保持するため、結果としてサイトがダウンする可能性があります。

この問題は、HAペアの両方のノードにVMACを構成することで解決できます。これにより、両方のノードが同一のMACアドレスを持つことになります。したがって、フェイルオーバーが発生し

でも、セカンダリノードのMACアドレスは変更されず、外部デバイス上のARPテーブルを更新する必要がなくなります。

VMACの構成は2段階のプロセスです。

1. SDX管理サービスでVMACを構成します。インターフェースまたはLAチャネルにVRIDを追加します。 [SDX管理サービスでVMACを構成する](#)。
2. CitrixインスタンスでVMACを構成します。詳細については、 [チャネルでVMACを構成するグループサポート](#)記事を参照してください。

SDX管理サービスでVMACを構成する

VMACを構成するには、管理サービスからインターフェースまたはLAチャネルにIPv4またはIPv6 VRIDを追加します。管理サービスは内部的にVMACを生成します。NetScalerインスタンスでアクティブ-アクティブモードを構成する際に、同じVRIDを指定します。このアクティブ-アクティブ構成は、Mellanoxインターフェースではサポートされていません。

以下の点に留意してください。

1. 管理サービスからVRIDを追加し、NetScalerインスタンスで同じVRIDを指定します。
NetScalerインスタンスに直接VRIDを追加した場合、インスタンスは宛先MACアドレスとしてVMACアドレスを持つパケットを受信できません。
2. 同じSDXアプライアンスで実行されている異なるインスタンスで、同じVRIDを使用することはできません。
3. インスタンスの実行中に、インスタンスに割り当てられたインターフェースのVRIDを追加または削除できます。
4. アクティブ/アクティブ構成では、インスタンスに割り当てられたインターフェースに対して複数のVRIDを指定できます。アクティブ/アクティブ展開は、Mellanoxインターフェースではサポートされていません。
5. 10Gインターフェースでは最大86個のVMACが、1Gインターフェースでは最大16個のVMACが許可されます。これ以上VMACフィルターが利用できない場合は、別のインスタンスのVRIDの数を減らしてください。

NetScaler VPXインスタンスを追加する際にVRIDを追加することも、既存のNetScalerインスタンスを変更してVRIDを追加することもできます。

インターフェースまたはLAチャネルにIPv4またはIPv6 VRIDを追加するには

1. SDXでVPXインスタンスを追加する際に、**「Network Settings」の下にある「Data Interfaces」**を選択します。SDXでVPXインスタンスを追加する方法の詳細については、「[NetScalerインスタンスの追加](#)」を参照してください。
2. **「Interfaces」**ドロップダウンメニューから、インターフェースまたはLAチャネルを選択します。
3. VMAC設定で、次の値のいずれかまたは両方を設定します。
 - VRID IPv4—VMACを識別するIPv4 VRID。指定可能な値：1～255。
 - VRID IPv6—VMACを識別するIPv6 VRID。指定可能な値：1～255。注：複数のVRIDを区切るにはコンマを使用します。例：12,24。
4. **「Add」**をクリックして、VMAC設定をインターフェースに追加します。
5. **「Finish」**をクリックし、次に「Close」**をクリックします。



インスタンスがすでにプロビジョニングされている場合は、IPv4またはIPv6 VRIDを追加するには、次の手順に従います。

1. SDX管理サービスから、**「Configuration」>「NetScaler」>「Instances」**に移動します。
2. インスタンスを選択し、**「Edit」**をクリックします。
3. 「データインターフェース」の下で、インターフェースを選択し、「編集」をクリックします。
4. VMAC設定の下で、VRID値を設定します。「追加」をクリックし、その後「完了」をクリックします。

SDXアプライアンスのNetScalerインスタンスで管理パーティションを設定するためのパーティションMACアドレスを生成する

NetScaler SDXアプライアンス上のNetScalerインスタンスは、管理パーティションと呼ばれる論理エンティティに分割できます。各パーティションは、個別のNetScalerインスタンスとして設定および使用できます。管理パーティションの詳細については、「[管理パーティション](#)」を参照してください。

共有VLAN構成で管理パーティションを使用するには、各パーティションに仮想MACアドレスが必要です。このような仮想MACアドレスはパーティションMAC (PMAC) アドレスと呼ばれ、共有VLANで受信したトラフィックを分類するために使用されます。このPMACアドレスは、そのパーティションにバインドされているすべての共有VLANで使われます。

管理パーティションを使用する前に、Management Serviceユーザーインターフェイスを使用してPMACアドレスを生成および設定します。Management Serviceでは、次の方法でパーティションMACアドレスを生成できます。

- ベースMACアドレスを使用する
- カスタムMACアドレスを指定する
- MACアドレスをランダムに生成する

注 パーティションMACアドレスを生成した後、管理パーティションを設定する前にNetScalerインスタンスを再起動する必要があります。

ベースMACアドレスを使用してパーティションMACアドレスを生成するには：

1. **Configuration**タブの左ペインで、**NetScaler**を展開し、**Instances**をクリックします。
2. **Instances**ペインで、パーティションMACアドレスを生成するNetScalerインスタンスを選択します。
3. **Action**ドロップダウンリストで、**Partition MACs**をクリックします。
4. **Partition MACs**ペインで、**Generate**をクリックします。
5. **Generate Partition MACs**ダイアログボックスの**Generation Method**セクションで、**Using Base Address**を選択します。
6. **Base MAC Address**フィールドに、ベースMACアドレスを入力します。
7. **Increment By**フィールドに、後続のMACアドレスごとにベースMACアドレスをインクリメントする値を入力します。たとえば、ベースMACアドレスを00:A1:C9:11:C8:11、増分値を2と指定した場合、次のMACアドレスは00:A1:C9:11:C8:13として生成されます。
8. **Count**フィールドに、生成するパーティションMACアドレスの数を入力します。
9. **Generate**をクリックします。

カスタムMACアドレスを指定してパーティションMACアドレスを生成するには：

1. **Configuration**タブの左ペインで、**NetScaler**を展開し、**Instances**をクリックします。
2. **Instances**ペインで、パーティションMACアドレスを生成するNetScalerインスタンスを選択します。

3. **Action**ドロップダウンリストで、**Partition MACs**をクリックします。
4. **Partition MACs**ペインで、**Generate**をクリックします。
5. **Generate Partition MACs**ダイアログボックスの**Generation Method**セクションで、**User Specified**を選択します。
6. **MAC Addresses**フィールドに、MACアドレスを入力します。
7. ****+****アイコンをクリックし、次のMACアドレスを入力します。さらにカスタムMACアドレスを指定するには、繰り返します。
8. **Generate**をクリックします。

パーティションMACアドレスをランダムに生成するには：

1. **Configuration**タブの左ペインで、**NetScaler**を展開し、**Instances**をクリックします。
2. **Instances**ペインで、パーティションMACアドレスを生成するNetScalerインスタンスを選択します。
3. 「**Action**」ドロップダウンリストで、「**Partition MACs**」をクリックします。
4. 「**Partition MACs**」ペインで、「**Generate**」をクリックします。
5. 「**Generate Partition MACs**」ダイアログボックスの「**Generation Method**」セクションで、「**Random**」を選択します。
6. 「**Count**」フィールドに、生成するパーティションMACアドレスの数を入力します。
7. 「**Generate**」をクリックします。

SDXアプライアンスでパーティションMACアドレスを生成した後、生成されたパーティションMACアドレスを使用してNetScalerインスタンス上の管理パーティションを構成します。

VPXインスタンスの変更管理

管理サービスからNetScaler VPXインスタンスの構成に対する変更を追跡できます。詳細ペインには、デバイス名とIPアドレス、最終更新日時が表示されます。また、保存された構成と実行中の構成の間に差異があるかどうか也表示されます。デバイスを選択すると、その実行中の構成、保存された構成、構成変更の履歴、およびアップグレード前後の構成の差異を表示できます。VPXインスタンスの構成をローカルコンピューターにダウンロードできます。デフォルトでは、管理サービスは24時間ごとにすべてのインスタンスをポーリングしますが、この間隔は変更できます。既存の構成ファイルからコマンドをコピーして監査テンプレートを作成できます。このテンプレートを使用して、インスタンスの構成の変更を検出し、必要に応じて修正措置を講じることができます。

VPXインスタンスの変更管理を表示するには

1. **Configuration** タブで、**NetScaler > Change Management** に移動します。
2. **Change Management** ペインで VPX インスタンスを選択し、**Action** リストから次のいずれかを選択します。
 - **Running Configuration**（実行中の構成） — 選択した VPX インスタンスの実行中の構成を新しいウィンドウに表示します。
 - **Saved Configuration**（保存された構成） — 選択した VPX インスタンスの保存された構成を新しいウィンドウに表示します。
 - **Saved Vs. Running Diff**（保存済みと実行中の差異） — 保存された構成、実行中の構成、および修正コマンド（差異）を表示します。
 - **Revision History Diff**（リビジョン履歴の差異） — ベース構成ファイルと2番目の構成ファイルの差異を表示します。
 - **Pre vs. Post Upgrade Diff**（アップグレード前後の差異） — アップグレード前後の構成の差異と、修正コマンド（差異）を表示します。
 - **Template Diff**（テンプレートの差異） — 保存された構成または実行中の構成とテンプレートの差異を表示します。この差異はバッチファイルとして保存できます。テンプレートの構成をインスタンスに適用するには、このバッチファイルをインスタンスに適用します。
 - **Download**（ダウンロード） — 選択した VPX インスタンスの構成をダウンロードし、ローカルデバイスに保存します。

NetScaler インスタンスの構成の更新をポーリングするには

1. **Configuration** タブで、**NetScaler > Change Management** に移動します。
2. **Change Management** ペインで、**Action** リストから次のいずれかを選択します。
 - **今すぐポーリング** — 管理サービスは、アプライアンスにインストールされている VPX インスタンスの構成 (ns.conf) の更新を直ちにポーリングします。
 - **ポーリング間隔の構成** — 管理サービスがアプライアンスにインストールされている VPX インスタンスの構成 (ns.conf) の更新をポーリングするまでの時間。デフォルトのポーリング間隔は24時間です。

NetScaler インスタンスの監査テンプレートを構成するには

1. 既存の構成ファイルを開き、そのコマンドリストをコピーします。
2. 「**構成**」タブで、「**NetScaler > 変更管理 > 監査テンプレート**」に移動します。
3. 詳細ペインで、「**追加**」をクリックします。

4. 「**テンプレートの追加**」ダイアログボックスで、テンプレートの名前と説明を追加します。
5. 「**コマンド**」テキストボックスに、構成ファイルからコピーしたコマンドリストを貼り付けます。
6. 「**作成**」をクリックし、次に「**閉じる**」をクリックします。

NetScalerインスタンスの監視

Management Serviceユーザーインターフェースの監視ページには、アプライアンスのパフォーマンスと、アプライアンスにプロビジョニングされたVPXインスタンスの概要が表示されます。NetScalerインスタンスをプロビジョニングおよび構成した後、NetScalerインスタンスを監視するためのさまざまなタスクを実行できます。

VPXインスタンスのプロパティを表示する

Management Serviceユーザーインターフェースには、SDXアプライアンスにプロビジョニングされたすべてのVPXインスタンスのリストと説明が表示されます。**NetScalerインスタンス**ペインを使用して、インスタンス名とIPアドレス、CPUとメモリの使用率、スループット、インスタンスに割り当てられた合計メモリなどの詳細を表示します。

VPXインスタンスのIPアドレスをクリックすると、そのインスタンスの構成ユーティリティ (GUI) が新しいタブまたはブラウザで開きます。

VPXインスタンスのプロパティを表示するには

1. 「Configuration」タブの左ペインで、「NetScaler Configuration」を展開し、「Instances」をクリックします。注: VPXインスタンスのプロパティは、「Home」タブからも表示できます。
2. NetScalerインスタンスペインで、NetScalerインスタンスについて以下の詳細を表示できます。
 - **名前:** プロビジョニング中にNetScalerインスタンスに割り当てられたホスト名。
 - **VMの状態:** 仮想マシンの状態。
 - **NetScalerの状態:** NetScalerインスタンスの状態。
 - **IPアドレス:** NetScalerインスタンスのIPアドレス。IPアドレスをクリックすると、このインスタンスのGUIが新しいタブまたはブラウザで開きます。
 - **Rx (Mbps):** NetScalerインスタンスで受信されたパケット。
 - **Tx (Mbps):** NetScalerインスタンスによって送信されたパケット。
 - **HTTP要求/秒:** NetScalerインスタンスで毎秒受信されるHTTP要求の合計数。
 - **CPU使用率 (%):** NetScalerでのCPU使用率のパーセンテージ。

- **メモリ使用率 (%):** NetScalerでのメモリ使用率のパーセンテージ。
3. NetScalerインスタンス名の横にある矢印をクリックすると、そのインスタンスのプロパティを表示できます。また、**すべて展開**をクリックすると、すべてのNetScalerインスタンスのプロパティを表示できます。以下のプロパティを表示できます。
- **ネットマスク:** NetScalerインスタンスのネットマスクIPアドレス。
 - **ゲートウェイ:** デフォルトゲートウェイのIPアドレス。これは、インスタンスがインストールされているサブネットの外部にトラフィックを転送するルーターです。
 - **1秒あたりのパケット数:** 毎秒通過するパケットの総数。
 - **NIC:** NetScalerインスタンスで使用されるNICの名前と、各インターフェイスに割り当てられた仮想機能。
 - **バージョン:** インスタンスで現在実行されているNetScalerソフトウェアのビルドバージョン、ビルド日付、および時刻。
 - **ホスト名:** NetScalerインスタンスのホスト名。
 - **合計メモリ (GB):** NetScalerインスタンスに割り当てられている合計メモリ。
 - **スループット (Mbps):** NetScalerインスタンスの合計スループット。
 - **稼働開始:** インスタンスが継続的にUP状態になってからの日付と時刻。
 - **SSLチップ:** インスタンスに割り当てられているSSLチップの総数。
 - **ピアIPアドレス:** HAセットアップの場合、このNetScalerインスタンスのピアのIPアドレス。
 - **ステータス:** NetScalerインスタンスで実行されている操作のステータス。たとえば、インスタンスからのインベントリが完了したかどうかのステータスなど。
 - **HA Master State:** デバイスの状態。この状態は、インスタンスがスタンドアロンまたはプライマリ設定で構成されているか、高可用性設定の一部であるかを示します。高可用性設定では、プライマリモードかセカンダリモードかも表示されます。
 - **HA Sync Status:** 有効または無効など、HA同期ステータスのモード。
 - **Description:** NetScalerインスタンスのプロビジョニング時に入力された説明。

注:

認証失敗によりADCインスタンスがサービス停止になった場合、以下の条件が満たされると、インスタンスの状態の色がグレーに変わります。

- インスタンスCLIを使用してADCインスタンスのパスワードが直接変更された。

- そのパスワードが、Management Serviceに保存されているインスタンス管理者プロファイルのパスワードと一致しない。
- インスタンスを初めて再起動した後、以前のセッションが失われる。

通常、インスタンスがサービス停止になると、インスタンスの状態の色は黄色になります。インスタンスを回復するには、次のいずれかを実行します。

- インスタンスCLIから、インスタンスのパスワードをインスタンスの管理者プロファイルのパスワードと一致するように変更します。その後、Management Serviceからインスタンスを再検出します。
- ADCインスタンスの現在のパスワードと同じパスワードで管理者プロファイルを作成します。その後、新しい管理者プロファイルでADCインスタンスを更新します。

NetScalerインスタンスの実行中および保存済み構成を表示する

Management Serviceを使用すると、NetScalerインスタンスの現在実行中の構成を表示できます。NetScalerインスタンスの保存済み構成と、構成が保存された時刻も表示できます。

NetScalerインスタンスの実行中および保存済み構成を表示するには

1. 「Configuration」タブの左ペインで、「NetScaler Configuration」を展開し、「Instances」をクリックします。
2. 「NetScaler instances」ペインで、実行中または保存済みの構成を表示するNetScalerインスタンスをクリックします。
3. 実行中の構成を表示するには「Running Configuration」をクリックし、保存済みの構成を表示するには「Saved Configuration」をクリックします。
4. 「NetScaler Running Config」ウィンドウまたは「NetScaler Saved Config」ウィンドウで、NetScalerインスタンスの実行中または保存済みの構成を表示できます。

NetScalerインスタンスをPingする

Management ServiceからNetScalerインスタンスをPingして、デバイスに到達可能かどうかを確認できます。

NetScalerインスタンスをPingするには

1. 「Configuration」タブの左ペインで、「NetScaler Configuration」を展開し、「Instances」をクリックします。

2. 「NetScaler instances」 ペインで、PingするNetScalerインスタンスをクリックし、「Ping」をクリックします。「Ping」メッセージボックスで、Pingが成功したかどうかを確認できます。

NetScalerインスタンスのルートをトレースする

Management ServiceからNetScalerインスタンスへのパケットのルートを、インスタンスに到達するために使用されたホップ数を特定することでトレースできます。

NetScalerインスタンスのルートをトレースするには

1. 「Configuration」 タブの左ペインで、「NetScaler Configuration」を展開し、「Instances」をクリックします。
2. 「NetScaler instances」 ペインで、トレースするNetScalerインスタンスをクリックし、「TraceRoute」をクリックします。「Traceroute」メッセージボックスで、NetScalerへのルートを確認できます。

NetScalerインスタンスを再検出する

NetScalerインスタンスの最新の状態と構成を表示する必要がある場合は、NetScalerインスタンスを再検出できます。

再検出中に、Management Serviceは構成を取得します。デフォルトでは、Management Serviceは30分ごとにデバイスの再検出をスケジュールします。

NetScalerインスタンスを再検出するには

1. 「Configuration」 タブの左側のペインで、「NetScaler Configuration」を展開し、「Instances」をクリックします。
2. 「NetScaler instances」 ペインで、再検出するNetScalerインスタンスをクリックし、「Rediscover」をクリックします。
3. 確認メッセージボックスで、「Yes」をクリックします。

ログを使用して操作とイベントを監視する

監査ログとタスクログを使用して、Management Service および NetScaler SDX インスタンスで実行された操作を監視します。イベントログを使用して、Management Service および Citrix Hypervisor で実行されたタスクのすべてのイベントを追跡することもできます。

監査ログを表示する

Management Service を使用して実行されたすべての操作は、アプライアンスデータベースにログ記録されます。監査ログを使用して、Management Service ユーザーが実行した操作、日付と時刻、および各操作の成功または失敗のステータスを表示できます。また、適切な列見出しをクリックすることで、ユーザー、操作、監査時刻、ステータスなどで詳細を並べ替えることもできます。

監査ログペインではページネーションがサポートされています。1 ページに表示するレコード数を選択します。デフォルトでは、1 ページに 25 件のレコードが表示されます。

監査ログを表示するには、次の手順に従います。

1. ナビゲーションペインで、[監査ログ](#)を展開し、[監査ログ](#)をクリックします。
2. 監査ログペインで、次の詳細を表示できます。
 - **ユーザー名:** 操作を実行した Management Service ユーザー。
 - **IP アドレス:** 操作が実行されたシステムの IP アドレス。
 - **ポート:** 操作が実行されたときにシステムが稼働していたポート。
 - **リソースタイプ:** xen_vpx_image や login など、操作の実行に使用されたリソースのタイプ。
 - **リソース名:** vpx_image_name やログインに使用されたユーザー名など、操作の実行に使用されたリソースの名前。
 - **監査時刻:** 監査ログが生成された時刻。
 - **操作:** add、delete、log out など、実行されたタスク。
 - **ステータス:** 監査のステータス（成功または失敗など）。

- **メッセージ:** 操作が失敗した場合の失敗の原因を説明するメッセージ、および操作が成功した場合のタスクのステータス（完了など）。

3. 特定のフィールドでログをソートするには、列の見出しをクリックします。

タスクログの表示

タスクログを使用して、NetScalerインスタンスでManagement Serviceによって実行される、インスタンスのアップグレードやSSL証明書のインストールなどのタスクを表示および追跡します。タスクログでは、タスクが進行中であるか、失敗したか、成功したかを確認できます。

タスクログペインではページネーションがサポートされています。1ページに表示するレコード数を選択します。デフォルトでは、1ページに25レコードが表示されます。

タスクログを表示するには、次の手順に従います。

1. ナビゲーションペインで、**タスクログ**を展開し、**タスクログ**をクリックします。
2. ペインで、次の詳細を表示できます。
 - **名前:** 実行中またはすでに実行されたタスクの名前。
 - **ステータス:** タスクのステータス（進行中、完了、失敗など）。
 - **実行者:** 操作を実行したManagement Serviceユーザー。
 - **開始時刻:** タスクが開始された時刻。
 - **終了時刻:** タスクが終了した時刻。

タスクデバイスログの表示

タスクデバイスログを使用して、各SDXインスタンスで実行されているタスクを表示および追跡します。タスクデバイスログを使用すると、タスクが進行中であるか、失敗したか、成功したかを確認できます。また、タスクが実行されているインスタンスのIPアドレスも表示されます。

タスクデバイスログを表示するには、次の手順に従います。

1. ナビゲーションペインで、**Diagnostics**を展開し、**Task Log**をクリックします。
2. **Task Log**ペインで、タスクをダブルクリックしてタスクデバイスの詳細を表示します。
3. **Task Device Log**ペインで、特定のフィールドでログをソートするには、列の見出しをクリックします。

タスクコマンドログの表示

タスクコマンドログを使用して、NetScalerインスタンスで実行されたタスクの各コマンドのステータスを表示します。タスクコマンドログを使用すると、コマンドが正常に実行されたか、失敗したかを確認できます。また、実行されたコマンドと、コマンドが失敗した理由も表示されます。

タスクコマンドログを表示するには、次の手順に従います。

1. ナビゲーションペインで、**Diagnostics**を展開し、**Task Log**をクリックします。
2. **Task Log**ペインで、タスクをダブルクリックしてタスクデバイスの詳細を表示します。
3. **Task Device Log**ペインで、タスクをダブルクリックしてタスクコマンドの詳細を表示します。
4. **Task Command Log**ペインで、特定のフィールドでログをソートするには、列の見出しをクリックします。

イベントの表示

Management Serviceユーザーインターフェイスの**Events**ペインを使用して、Management Serviceで実行されたタスクに対してManagement Serviceによって生成されたイベントを監視します。

イベントを表示するには、次の手順に従います。

1. 「**System > Events**」に移動します。
2. 「**Events**」ペインで、以下の詳細を表示できます。
 - **重大度**: イベントの重大度。重大、主要、軽微、クリア、情報などがあります。
 - **ソース**: イベントが生成されたIPアドレス。
 - **日付**: イベントが生成された日付。
 - **カテゴリ**: PolicyFailedやDeviceConfigChangeなどのイベントのカテゴリ。
 - **メッセージ**: イベントを説明するメッセージ。
3. 特定のフィールドでイベントをソートするには、列の見出しをクリックします。

NetScaler SDXアプライアンスのユースケース

ネットワークコンポーネント（ファイアウォールやアプリケーションデリバリーコントローラーなど）の場合、マルチテナンシーのサポートは、歴史的に単一のデバイスを複数の論理パーティションに分割する機能を含んでいました。このアプローチにより、多数の個別のデバイスを必要とせずに、テナントごとに異なるポリシーセットを実装できます。しかし、従来の方法では、達成される分離の度合いに関して、厳しく制限されていました。

設計上、SDXアプライアンスは同じ制限を受けません。SDXアーキテクチャでは、各インスタンスは、専用のNetScalerカーネル、CPUリソース、メモリリソース、アドレス空間、帯域幅割り当てを持つ個別の仮想マシン（VM）として実行されます。SDXアプライアンス上のネットワークI/Oは、システム全体のパフォーマンスを維持するだけでなく、各テナントのデータプレーンおよび管理プレーンのトラフィックを完全に分離することを可能にします。管理プレーンには0/xインターフェースが含まれます。データプレーンには1/xおよび10/xインターフェースが含まれます。データプレーンは管理プレーンとしても使用できます。

SDXアプライアンスの主なユースケースは、統合に関連しており、管理の分離を維持しながら必要なネットワークの数を削減することです。以下に、基本的な統合シナリオを示します。

- Management ServiceとNetScalerインスタンスが同じネットワークにある場合の統合。
- Management ServiceとNetScalerインスタンスが異なるネットワークにあるが、すべてのインスタンスが同じネットワークにある場合の統合。
- セキュリティをまたいだ統合。
- 各インスタンスに専用インターフェースを持つ統合。
- 複数のインスタンスによる物理ポートの共有を伴う統合。

Management Service と NetScaler インスタンスが同じネットワークにある場合の統合

SDX アプライアンスにおける統合の単純なケースは、Management Service と NetScaler インスタンスを同じネットワークの一部として構成することです。このユースケースは、次の場合に適用されます。

- アプライアンス管理者とインスタンス管理者が同一である場合。

- 組織のコンプライアンス要件で、Management Service と異なるインスタンスの NSIP アドレスに個別の管理ネットワークが必要であると指定されていない場合。

インスタンスは同じネットワーク（管理トラフィック用）にプロビジョニングできます。VIP アドレスは異なるネットワーク（データトラフィック用）に構成でき、したがって異なるセキュリティゾーンに配置できます。

次の例では、Management Service と NetScaler インスタンスは 10.1.1.x ネットワークの一部です。インターフェイス 0/1 と 0/2 は管理インターフェイス、1/1 から 1/8 は 1G データインターフェイス、10/1 から 10/4 は 10G データインターフェイスです。各インスタンスには専用の物理インターフェイスがあります。したがって、インスタンスの数はアプライアンスで利用可能な物理インターフェイスの数に制限されます。デフォルトでは、SDX アプライアンスの各インターフェイスで VLAN フィルタリングが有効になっています。VLAN の数は、1G インターフェイスでは 32、10G インターフェイスでは 63 に制限されています。VLAN フィルタリングは各インターフェイスで有効/無効にできます。VLAN フィルタリングを無効にすると、各インスタンスのインターフェイスごとに最大 4096 の VLAN を構成できます。この例では、各インスタンスに専用インターフェイスがあるため、VLAN フィルタリングは不要です。VLAN フィルタリングの詳細については、「[Manage and monitor the SDX appliance](#)」の「**VLAN フィルタリング**」セクションを参照してください。

次の図は、上記のユースケースを示しています。

図 1. Management Service とインスタンスの NSIP が同じネットワークにある SDX アプライアンスのネットワークトポロジ



次の表に、上記の例で NetScaler インスタンス 1 をプロビジョニングするために使用されるパラメータの名前と値を示します。

パラメータ名	インスタンス 1 の値
名前	vpx8
IP アドレス	10.1.1.2
ネットマスク	255.255.255.0
ゲートウェイ	10.1.1.1
XVAファイル	NS-VPX-XEN-10.0-51.308.a_nc.xva
機能ライセンス	プラチナ

パラメータ名	インスタンス 1 の値
管理者プロファイル	ns_nsroot_profile
ユーザー名	vpx8
パスワード	Sdx1
パスワードの確認	Sdx1
Shell/Sftp/Scp アクセス	はい
合計メモリ (MB)	2048
#SSL チップ	1
スループット (Mbps)	1000
1秒あたりのパケット数	1000000
CPU	共有
インターフェース	0/1 および 1/1

この例に示すように NetScaler インスタンス 1 をプロビジョニングする

1. タブのナビゲーションペインで、 を展開し、 をクリックします。
2. ペインで、 をクリックします。
3. で、ウィザードの指示に従って、前の表に示されているパラメータ値を指定します。
4. をクリックし、 をクリックします。プロビジョニングした NetScaler インスタンスが ペインに表示されます。

管理サービスとNetScalerインスタンスが異なるネットワークにある場合の統合

特定のケースでは、アプライアンス管理者は他の管理者に個々のインスタンスで管理タスクを実行させる場合があります。これは、個々のインスタンス管理者にそのインスタンスのみへのログイン権限を与えることで安全に行うことができます。しかし、セキュリティ上の理由から、アプライアンス管理者はインスタンスを管理サービスと同じネットワークに置くことを望まない場合があ

ります。これはサービスプロバイダー環境で一般的なシナリオであり、仮想化やクラウドアーキテクチャを採用する企業でもますます一般的になっています。

次の例では、管理サービスは10.1.1.xネットワークにあり、NetScalerインスタンスは10.1.2.xネットワークにあります。インターフェイス0/1と0/2は管理インターフェイス、1/1から1/8は1Gデータインターフェイス、10/1から10/4は10Gデータインターフェイスです。各インスタンスには専用の管理者と専用の物理インターフェイスがあります。したがって、インスタンスの数はアプライアンスで利用可能な物理インターフェイスの数に制限されます。各インスタンスには専用のインターフェイスがあるため、VLANフィルタリングは不要です。オプションで、VLANフィルタリングを無効にして、インターフェイスごとにインスタンスあたり最大4096個のVLANを構成できます。この例では、インスタンスが物理インターフェイスを共有しておらず、タグ付きVLANがないため、NSVLANを構成する必要はありません。NSVLANの詳細については、「[NetScalerインスタンスの追加](#)」を参照してください。

次の図は、上記のユースケースを示しています。

図1. 管理サービスとインスタンスのNSIPが異なるネットワークにあるSDXアプライアンスのネットワークトポロジ



アプライアンス管理者として、管理サービスとSDXアプライアンス上のNSIPアドレス間のトラフィックをアプライアンス内に留めることができます。または、たとえば、トラフィックを外部ファイアウォールやその他のセキュリティ仲介を介してアプライアンスに戻したい場合は、デバイスからトラフィックを強制的に出すこともできます。

次の表は、この例でNetScalerインスタンス1をプロビジョニングするために使用されるパラメータの名前と値を示しています。

パラメータ名	インスタンス1の値
名前	vpx1
IPアドレス	10.1.2.2
ネットマスク	255.255.255.0
ゲートウェイ	10.1.2.1
XVAファイル	NS-VPX-XEN-10.0-51.308.a_nc.xva
機能ライセンス	プラチナ

パラメータ名	インスタンス1の値
管理者プロファイル	ns_nsroot_profile
ユーザー名	vpx1
パスワード	Sdx1
パスワードの確認	Sdx1
シェル/SFTP/SCP アクセス	はい
合計メモリ (MB)	2048
#SSL チップ	1
スループット (Mbps)	1000
1秒あたりのパケット数	1000000
CPU	共有
インターフェース	0/2 および 1/1

この例に示すように、NetScaler インスタンス 1 をプロビジョニングするには

1. 「**Configuration**」 タブのナビゲーションペインで、「**NetScaler Configuration**」を展開し、「**Instances**」をクリックします。
2. NetScaler インスタンスペインで、「**Add**」をクリックします。
3. 「**Provision NetScaler Wizard**」で、ウィザードの指示に従って、前の表に示されている値にパラメータを設定します。
4. 「**Create**」をクリックし、次に「**Close**」をクリックします。プロビジョニングしたNetScaler インスタンスがNetScaler インスタンスペインに表示されます。

セキュリティゾーン間の統合

SDX アプライアンスは、セキュリティゾーン間の統合によく使用されます。DMZは、攻撃者がDMZにのみアクセスできるため、組織の内部ネットワークにセキュリティの追加レイヤーを追加します。組織の内部ネットワークにはアクセスできません。コンプライアンス要件の厳しい環境では、DMZと内部ネットワークの両方にVIPアドレスを持つ単一のNetScaler インスタンスは許容さ

れません。SDXを使用すると、DMZでVIPアドレスをホストするインスタンスと、内部ネットワークでVIPアドレスをホストする他のインスタンスをプロビジョニングできます。

セキュリティゾーンごとに個別の管理ネットワークが必要になる場合があります。DMZ内のインスタンスのNSIPアドレスは、1つのネットワークに配置できます。内部ネットワークにVIPを持つインスタンスのNSIPアドレスは、別の管理ネットワークに配置できます。また、多くの場合、Management Serviceとインスタンス間の通信は、ルーターなどの外部デバイスを介してルーティングする必要がある場合があります。ファイアウォールに送信されるトラフィックを制御し、トラフィックをログに記録するようにファイアウォールポリシーを構成できます。

SDXアプライアンスには、2つの管理インターフェイス (0/1および0/2) と、モデルに応じて最大8つの1Gデータポートおよび8つの10Gデータポートがあります。データポートを管理ポートとして使用することもできます (たとえば、タグ付きVLANを構成する必要がある場合など。管理インターフェイスではタグ付けが許可されていないため)。その場合、Management Serviceからのトラフィックはアプライアンスを離れてからアプライアンスに戻る必要があります。このトラフィックをルーティングするか、オプションでインスタンスに割り当てられたインターフェイスでNSVLANを指定できます。管理インターフェイスがインスタンスとManagement Serviceの間に共通である場合、両者間のトラフィックをルーティングする必要はありません。ただし、セットアップで明示的に必要な場合は、トラフィックをルーティングできます。

注: タグ付けはCitrix Hypervisorバージョン6.0でサポートされています。

各インスタンスに専用インターフェースを使用した統合

次の例では、インスタンスは複数のネットワークの一部です。インターフェイス0/1は、内部10.1.1.xネットワークの一部である管理サービスに割り当てられています。NetScalerインスタンス2と3は10.1.200.xネットワーク (VLAN 100) の一部です。NetScalerインスタンス4と5は10.1.3.xネットワーク (VLAN 200) の一部です。

必要に応じて、すべてのインスタンスでNSVLANを構成できます。

次の図は、前述のユースケースを示しています。

図1. 複数のネットワークにNetScalerインスタンスを持つSDXアプライアンスのネットワークトポロジ



SDXアプライアンスはスイッチに接続されています。アプライアンスのポート1/1が接続されているスイッチポートに、VLAN ID 100と200が構成されていることを確認してください。

次の表に、この例でNetScalerインスタンス5と3をプロビジョニングするために使用されるパラメーターの名前と値を示します。

パラメーター名	インスタンス5の値	インスタンス3の値
名前	vpx5	vpx3
IPアドレス	10.1.3.2	10.1.200.2
ネットマスク	255.255.255.0	255.255.255.240
ゲートウェイ	10.1.3.1	10.1.200.1
XVAファイル	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
機能ライセンス	プラチナ	プラチナ
管理者プロファイル	ns_nsroot_profile	ns_nsroot_profile
ユーザー名	vpx5	vpx3
パスワード	Sdx1	ルート
パスワードの確認	Sdx1	ルート
シェル/SFTP/SCPアクセス	はい	はい
合計メモリ (MB)	2048	2048
#SSLチップ	1	1
スループット (Mbps)	1000	1000
1秒あたりのパケット数	1000000	1000000
CPU	共有	共有
インターフェース	1/1 および 10/4	1/1 および 1/5
NSVLAN	200	100
追加 (インターフェース)	1/1	1/1
タグ付きインターフェース	タグ付きを選択	タグ付きを選択

この例に示すように、NetScaler インスタンス 5 と 3 をプロビジョニングするには

1. **Configuration** タブのナビゲーションペインで、**NetScaler Configuration** を展開し、**Instances** をクリックします。
2. NetScaler インスタンスペインで、**Add** をクリックします。
3. **Provision NetScaler Wizard** で、ウィザードの指示に従って、前の表に示されている値にパラメータを設定します。
4. 「作成」をクリックし、次に「閉じる」をクリックします。プロビジョニングしたNetScaler インスタンスが、NetScalerインスタンスペインに表示されます。

複数のインスタンスによる物理ポートの共有を伴う統合

必要に応じて、インターフェイスでVLANフィルタリングを有効または無効にできます。たとえば、インスタンスで100を超えるVLANを構成するには、そのインスタンスに専用の物理インターフェイスを割り当て、そのインターフェイスでVLANフィルタリングを無効にします。物理インターフェイスを共有するインスタンスではVLANフィルタリングを有効にして、あるインスタンスが別のインスタンスのトラフィックを見ることができないようにします。

注: VLANフィルタリングはアプライアンスのグローバル設定ではありません。インターフェイスでVLANフィルタリングを有効または無効にすると、その設定はそのインターフェイスに関連付けられているすべてのインスタンスに適用されます。VLANフィルタリングが無効になっている場合、最大4096個のVLANを構成できます。VLANフィルタリングが有効になっている場合、10Gインターフェイスでは最大63個のタグ付きVLAN、1Gインターフェイスでは最大32個のタグ付きVLANを構成できます。

次の例では、インスタンスは複数のネットワークの一部です。

- インターフェイス1/1は、すべてのインスタンスに管理インターフェイスとして割り当てられています。インターフェイス0/1は、内部10.1.1.xネットワークの一部であるManagement Serviceに割り当てられています。
- NetScalerインスタンス2と3は10.1.200.xネットワークにあり、インスタンス4、5、6、7は10.1.3.xネットワークにあります。インスタンス2と3はそれぞれ専用の物理インターフェイスを持っています。インスタンス4と7は物理インターフェイス1/7を共有し、インスタンス5と6は物理インターフェイス10/4を共有します。
- インターフェイス1/7でVLANフィルタリングが有効になっています。インスタンス4のトラフィックはVLAN 4用にタグ付けされ、インスタンス7のトラフィックはVLAN 7用にタグ付けされます。その結果、インスタンス4のトラフィックはインスタンス7には見えません。逆に、インスタンス7のトラフィックはインスタンス4には見えません。インターフェイス1/7では最大32個のVLANを構成できます。

- インターフェイス10/4ではVLANフィルタリングが無効になっているため、そのインターフェイスで最大4096個のVLANを構成できます。インスタンス5にはVLAN 500～599を、インスタンス6にはVLAN 600～699を構成します。インスタンス5はVLAN 600～699からのブロードキャストおよびマルチキャストトラフィックを見ることができますが、パケットはソフトウェアレベルで破棄されます。同様に、インスタンス6はVLAN 500～599からのブロードキャストおよびマルチキャストトラフィックを見ることができますが、パケットはソフトウェアレベルで破棄されます。

次の図は、上記のユースケースを示しています。

図1. Management ServiceとNetScalerインスタンスがネットワーク全体に分散されたSDXアプリケーションのネットワークトポロジ



次の表に、この例でNetScalerインスタンス7と4をプロビジョニングするために使用されるパラメータの名前と値を示します。

パラメータ名	インスタンス7の値	インスタンス4の値
名前	vpx7	vpx4
IPアドレス	10.1.3.7	10.1.3.4
ネットマスク	255.255.255.0	255.255.255.240
ゲートウェイ	10.1.3.1	10.1.3.1
XVAファイル	NS-VPX-XEN-10.0-51.308.a_nc.xva	NS-VPX-XEN-10.0-51.308.a_nc.xva
機能ライセンス	プラチナ	プラチナ
管理者プロファイル	ns_nsroot_profile	ns_nsroot_profile
ユーザー名	vpx4	vpx4
パスワード	Sdx1	Sdx1
パスワードの確認	Sdx1	Sdx1
シェル/SFTP/SCPアクセス	はい	はい
合計メモリ (MB)	2048	2048

パラメータ名	インスタンス7の値	インスタンス4の値
#SSLチップ	1	1
スループット (Mbps)	1000	1000
1秒あたりのパケット数	1000000	1000000
CPU	共有	共有
インターフェース	1/1 および 1/7	1/1 および 1/7
NSVLAN	200	200

この例でNetScalerインスタンス7と4をプロビジョニングするには

1. **Configuration**タブのナビゲーションペインで、NetScaler Configurationを展開し、**Instances**をクリックします。
2. NetScalerインスタンスペインで、**Add**をクリックします。
3. Provision NetScalerウィザードで、ウィザードの指示に従って、前の表に示されている値にパラメータを設定します。
4. **Create**をクリックし、次に**Close**をクリックします。プロビジョニングしたNetScalerインスタンスがNetScalerインスタンスペインに表示されます。

NITRO API

NetScaler SDX NITROプロトコルを使用すると、SDXアプライアンスをプログラムで構成および監視できます。

NITROは、Representational State Transfer (REST) インターフェースを介してその機能を公開します。そのため、NITROアプリケーションは任意のプログラミング言語で開発できます。また、Java、.NET、またはPythonで開発する必要があるアプリケーションの場合、NITROプロトコルは個別のソフトウェア開発キットとしてパッケージ化された関連ライブラリとして公開されています。

注: NITROを使用する前に、SDXアプライアンスの基本的な理解が必要です。

NITROプロトコルを使用するには、クライアントアプリケーションは以下を必要とします。

- SDXアプライアンスへのアクセス。
- RESTインターフェースを使用するには、SDXアプライアンスに対してHTTPまたはHTTPSリクエスト（JSON形式のペイロード）を生成するシステムが必要です。任意のプログラミング言語またはツールを使用できます。
- Javaクライアントの場合、Java Development Kit (JDK) 1.5以降のバージョンが利用可能なシステムが必要です。JDKは <http://www.oracle.com/technetwork/java/javase/downloads/index.html> からダウンロードできます。
- .NETクライアントの場合、.NET framework 3.5以降のバージョンが利用可能なシステムが必要です。.NET frameworkは<http://www.microsoft.com/downloads/en/default.aspx>からダウンロードできます。
- Pythonクライアントの場合、Python 2.7以降のバージョンとRequestsライブラリ（`<NITRO_SDK_HOME>/lib`で利用可能）がインストールされているシステムが必要です。

NITROパッケージの入手

NITROパッケージは、SDXアプライアンスの構成ユーティリティのダウンロードページでtarファイルとして提供されています。ファイルをダウンロードし、ローカルシステムのフォルダに展開する必要があります。このドキュメントでは、このフォルダを`<NITRO_SDK_HOME>`と呼びます。

このフォルダには、NITROライブラリが lib サブフォルダに含まれています。NITRO 機能にアクセスするには、ライブラリをクライアントアプリケーションのクラスパスに追加する必要があります。 \<NITRO_SDK_HOME> フォルダには、NITRO SDK を理解するのに役立つサンプルとドキュメントも含まれています。

注記:

```
<div id="sdx-nitro-obtain-con__li_5716E0FF34204411A267E100E8A92067">
```

The REST package contains only documentation for using the REST interfaces.

```
</div>
```

```
<div id="sdx-nitro-obtain-con__li_A72149DD47854CE9B82A5DA88B705828">
```

For the Python SDK, the library must be installed on the client path. For installation instructions, read the \<NITRO_SDK_HOME>/README.txt file.

```
</div>
```

.NET SDK

SDX NITRO API は、その API の範囲と目的に応じて、システム API と構成 API に分類されます。NITRO 操作のトラブルシューティングも行えます。

システムAPI

NITRO を使用するための最初のステップは、SDX アプライアンスとのセッションを確立し、管理者の資格情報を使用してセッションを認証することです。

アプライアンスのIPアドレスと、アプライアンスに接続するためのプロトコル（HTTPまたはHTTPS）を指定して、nitro_serviceクラスのオブジェクトを作成します。その後、このオブジェクトを使用して、管理者のユーザー名とパスワードを指定してアプライアンスにログオンします。

注: そのアプライアンスにユーザーアカウントが必要です。実行できる構成操作は、アカウントに割り当てられている管理ロールによって制限されます。

次のサンプルコードは、HTTPSプロトコルを使用してIPアドレス10.102.31.16を持つSDXアプライアンスに接続します。

```
//Specify the IP address of the appliance and service type

nitro_service nitroservice = new nitro_service ("10.102.31.16", "https");

//Specify the login credentials

nitroservice.login("nsroot", "verysecret");
```

注: アプライアンスでの今後のすべてのNITRO操作で、nitro_service オブジェクトを使用します。

アプライアンスから切断するには、次のようにlogout()メソッドを呼び出します。

```
nitroservice.logout();
```

構成API

NITROプロトコルは、SDXアプライアンスのリソースを構成するために使用できます。

リソースを構成するためのAPIは、com.citrix.sdx.nitro.resource.config.<resource_type>という形式のパッケージまたは名前空間にグループ化されています。これらのパッケージまたは名前空間のそれぞれには、そのリソースを構成するためのAPIを提供する<resource_type>という名前のクラスが含まれています。

例えば、NetScalerリソースには、com.citrix.sdx.nitro.resource.config.nsパッケージまたは名前空間があります。

リソースクラスは、他の操作を実行するためのAPIを提供します。これらの操作には、リソースの作成、リソースとリソースプロパティの取得、リソースの更新、リソースの削除、およびリソースに対する一括操作の実行が含まれます。

リソースの作成

SDXアプライアンス上にリソース（例：NetScalerインスタンス）を作成するには：

1. 対応するプロパティ名を使用して、リソースの必須プロパティの値を設定します。その結果、リソースに必要な詳細を含むリソースオブジェクトが作成されます。注：これらの値はクライアントにローカルに設定されます。オブジェクトがアップロードされるまで、これらの値はアプライアンスに反映されません。
2. 静的 add() メソッドを使用して、リソースオブジェクトをアプライアンスにアップロードします。

次のサンプルコードは、SDXアプライアンス上に「ns_instance」という名前のNetScalerインスタンスを作成します。

```
ns newns = new ns();

//Set the properties of the NetScaler locally

newns.name = "ns_instance";

newns.ip_address = "10.70.136.5";

newns.netmask = "255.255.255.0";

newns.gateway = "10.70.136.1";

newns.image_name = "nsvpx-9.3.45_nc.xva";

newns.profile_name = "ns_nsroot_profile";

newns.vm_memory_total = 2048;

newns.throughput = 1000;

newns.pps = 1000000;

newns.license = "Standard";

newns.username = "admin";

newns.password = "admin";
```

```
int number_of_interfaces = 2;

network_interface[] interface_array = new
network_interface[number_of_interfaces];

//Adding 10/1

interface_array[0] = new network_interface();

interface_array[0].port_name = "10/1";

//Adding 10/2

interface_array[1] = new network_interface();

interface_array[1].port_name = "10/2";

newns.network_interfaces = interface_array;

//Upload the NetScaler instance

ns result = ns.add(nitroservice, newns);
```

リソースの詳細を取得する

SDXアプライアンス上のリソースのプロパティを取得するには、次の手順を実行します。

1. `get()` メソッドを使用して、アプライアンスから構成を取得します。その結果、リソースオブジェクトが作成されます。
2. 対応するプロパティ名を使用して、オブジェクトから必要なプロパティを抽出します。

次のサンプルコードは、すべてのNetScaler®リソースの詳細を取得します。

```
//Retrieve the resource object from the SDX appliance

ns[] returned_ns = ns.get(nitroservice);


//Extract the properties of the resource from the object

Console.WriteLine(returned_ns[i].ip_address);

Console.WriteLine(returned_ns[i].netmask);
```

リソース統計を取得する

SDXアプライアンスは、その機能の使用状況に関する統計を収集します。これらの統計はNITROを使用して取得できます。

次のサンプルコードは、ID 123456a のNetScalerインスタンスの統計を取得します。

```
ns obj = new ns();

obj.id = "123456a";

ns stats = ns.get(nitroservice, obj);

Console.WriteLine("CPU Usage:" + stats.ns_cpu_usage);

Console.WriteLine("Memory Usage:" + stats.ns_memory_usage);

Console.WriteLine("Request rate/sec:" +stats.http_req);
```

リソースを更新する

アプライアンス上の既存のリソースのプロパティを更新するには、次の手順を実行します。

1. id プロパティを更新するリソースのIDに設定します。
2. リソースの必須プロパティの値を、対応するプロパティ名を使用して設定します。結果はリソースオブジェクトになります。注: これらの値はクライアント上でローカルに設定されません。オブジェクトがアップロードされるまで、これらの値はアプライアンスに反映されません。

3. update() メソッドを使用して、リソースオブジェクトをアプライアンスにアップロードします。

次のサンプルコードは、ID 123456a の NetScaler インスタンスの名前を「ns_instance_new」に更新します。

```
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated

update_obj.id = "123456a";

//Get existing NetScaler details

update_obj = ns.get(nitroservice, update_obj);

//Update the name of the NetScaler to "ns_instance_new" locally

update_obj.name = "ns_instance_new";

//Upload the updated NetScaler details

ns result = ns.update(nitroservice, update_obj);
```

リソースを削除する

既存のリソースを削除するには、削除するリソースの ID を引数として渡し、リソースクラスの静的メソッド delete() を呼び出します。

次のサンプルコードは、ID 1 の NetScaler インスタンスを削除します。

```
ns obj = new ns();

obj.id = "123456a";
```

```
ns.delete(nitroservice, obj);
```

一括操作

複数のリソースを同時に照会または変更できるため、ネットワークトラフィックを最小限に抑えることができます。たとえば、同じ操作で複数の NetScaler SDX アプライアンスを追加できます。

各リソースクラスには、リソースの追加、更新、削除のためにリソースの配列を受け取るメソッドがあります。一括操作を実行するには、各操作の詳細をローカルで指定し、その詳細を一度にサーバーに送信します。

一括操作内の一部の操作の失敗を考慮するために、NITRO では次のいずれかの動作を構成できます。

- ****終了。** **最初のエラーが発生すると、実行は停止します。エラーの前に実行されたコマンドはコミットされます。
- ****続行。** **一部のコマンドが失敗しても、リスト内のすべてのコマンドが実行されます。

注: アプライアンスとの接続を確立する際に、必要な動作を構成するには、`onerror` パラメータを `nitro_service()` メソッドで設定します。

次のサンプルコードは、1 回の操作で 2 つの ADC アプライアンスを追加します。

```
ns[] newns = new ns[2];

//Specify details of first NetScaler

newns[0] = new ns();

newns[0].name = "ns_instance1";

newns[0].ip_address = "10.70.136.5";

newns[0].netmask = "255.255.255.0";

newns[0].gateway = "10.70.136.1";

...
```

```
...

//Specify details of second NetScaler

newns[1] = new ns();

newns[1].name = "ns_instance2";

newns[1].ip_address = "10.70.136.8";

newns[1].netmask = "255.255.255.0";

newns[1].gateway = "10.70.136.1";

...

...

//upload the details of the ADC appliances to the NITRO server

ns[] result = ns.add(nitroservice, newns);
```

例外処理

エラーコードフィールドは、操作のステータスを示します。

- エラーコードが0の場合は、操作が成功したことを示します。
- ゼロ以外のエラーコードは、NITROリクエストの処理中にエラーが発生したことを示します。

エラーメッセージフィールドには、簡単な説明と障害の性質が記載されています。

`com.citrix.sdx.nitro.exception.nitro_exception`クラスは、NITRO APIの実行におけるすべての例外をキャッチします。例外に関する情報を取得するには、`getErrorCode()` メソッドを使用できます。

エラーコードの詳細については、`<NITRO_SDK_HOME>/doc` フォルダーにあるAPIリファレンスを参照してください。

REST Webサービス

REST（Representational State Transfer）は、クライアントとサーバー間のシンプルなHTTPリクエストとレスポンスに基づいたアーキテクチャスタイルです。RESTは、サーバー側のオブジェクトの状態を照会または変更するために使用されます。RESTでは、サーバー側はエンティティのセットとしてモデル化され、各エンティティは一意的URLによって識別されます。

各リソースには状態もあり、その状態に対して以下の操作を実行できます。

- **作成。** クライアントは、「コンテナ」リソース上に新しいサーバー側リソースを作成できます。コンテナリソースはフォルダ、子リソースはファイルまたはサブフォルダと考えることができます。呼び出し元のクライアントは、作成されるリソースの状態を提供します。状態は、XMLまたはJSON形式を使用してリクエストで指定できます。クライアントは、新しいオブジェクトを識別する一意のURLを指定することもできます。あるいは、サーバーが作成されたオブジェクトを識別する一意のURLを選択して返すこともできます。作成リクエストに使用されるHTTPメソッドはPOSTです。
- **読み取り。** クライアントは、HTTP GETメソッドでURLを指定することにより、リソースの状態を取得できます。レスポンスメッセージには、JSON形式で表現されたリソースの状態が含まれます。
- **更新。** PUT HTTPメソッドを使用して、オブジェクトを識別するURLと、JSONまたはXML形式の新しい状態を指定することにより、既存のリソースの状態を更新できます。
- **削除。** DELETE HTTPメソッドと、削除するリソースを識別するURLを使用することにより、サーバー上に存在するリソースを破棄できます。

これら4つのCRUD操作（作成、読み取り、更新、削除）に加えて、リソースは他の操作またはアクションをサポートできます。これらの操作はHTTP POSTメソッドを使用し、JSON形式のリクエストボディで実行する操作とその操作のパラメータを指定します。

SDX NITRO APIは、APIのスコープと目的に応じて、システムAPIと構成APIに分類されます。

システムAPI

NITROを使用するための最初のステップは、SDXアプライアンスとのセッションを確立し、管理者の資格情報を使用してセッションを認証することです。

ログインオブジェクトでユーザー名とパスワードを指定します。作成されたセッションIDは、セッション内のそれ以降のすべての操作のリクエストヘッダーで指定する必要があります。

注: そのアプライアンスにユーザーアカウントが必要です。実行できる構成は、アカウントに割り当てられた管理ロールによって制限されます。

HTTPSプロトコルを使用して、IPアドレス10.102.31.16のSDXアプライアンスに接続するには：

- **URL** `https://10.102.31.16/nitro/v2/config/login/`
- **HTTP メソッド** POST
- **リクエスト**

- **ヘッダー**

```
Content-Type:application/vnd.com.citrix.sdx.login+json
```

注: 以前のバージョンの NITRO でサポートされていた「application/x-www-form-urlencoded」などのコンテンツタイプも使用できます。ペイロードが以前のバージョンで使用されていたものと同じであることを確認してください。このドキュメントで提供されているペイロードは、コンテンツタイプが「application/vnd.com.citrix.sdx.login+json」の形式である場合にのみ適用されます。

- **ペイロード**

```
{  
  
  "login":  
  
  {  
  
    "username":"nsroot",  
  
    "password":"verysecret"  
  
  }  
  
}
```

- **応答ペイロード**

- **ヘッダー**

```
HTTP/1.0 201 Created
```

```
Set-Cookie:
```

```
NITRO_AUTH_TOKEN=##87305E9C51B06C848F0942; path=/nitro/v2
```

注: アプライアンスでの今後のすべての NITRO 操作でセッション ID を使用してください。

注: デフォルトでは、アプライアンスへの接続は30分間操作がないと期限切れになります。タイムアウト期間は、新しいタイムアウト期間（秒単位）を ログインオブジェクトで指定することで変更できます。たとえば、タイムアウト期間を60分に変更する場合、リクエストペイロードは次のようになります。

```
{  
  
  "login":  
  
  {  
  
    "username":"nsroot",  
  
    "password":"verysecret",  
  
    "timeout":3600  
  
  }  
  
}
```

操作のリクエストヘッダーにユーザー名とパスワードを指定することで、単一の操作を実行するためにアプライアンスに接続することもできます。たとえば、NetScaler インスタンスの作成中にアプライアンスに接続するには、次のようになります。

- URL
- HTTP メソッド
- リクエスト
 - ヘッダー

```
X-NITRO-USER:nsroot
```

```
X-NITRO-PASS:verysecret
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

- ペイロード

```
{  
  
  "ns":  
  
  {  
  
    ...  
  
  }  
  
}
```

- 応答。

- ヘッダー

```
HTTP/1.0 201 Created
```

アプライアンスから切断するには、DELETE メソッドを使用します。

- URL

- HTTP メソッド DELETE

- リクエスト

- ヘッダー

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.login+json
```

構成API

NITRO プロトコルは、SDX アプライアンスのリソースを構成するために使用できます。

各SDXリソースには、実行される操作の種類に応じて一意のURLが関連付けられています。構成操作のURLは次の形式です: `http://<IP>/nitro/v2/config/<resource_type>`

リソースの作成

SDX アプライアンス上でリソース (たとえば、NetScaler インスタンス) を作成するには、特定のリソースオブジェクトにリソース名とその他の関連引数を指定します。たとえば、vpx1 という名前の NetScaler インスタンスを作成するには:

- URL
- HTTP メソッド
- リクエスト
 - ヘッダー

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

- ペイロード

```
{
  "ns":
  {
    "name": "vpx1",
    "ip_address": "192.168.100.2",
    "netmask": "255.255.255.0",
    "gateway": "192.168.100.1",
    "image_name": "nsvpx-9.3-45_nc.xva",
    "vm_memory_total": 2048,
    "throughput": 1000,
    "pps": 1000000,
```

```
    "license": "Standard",

    "profile_name": "ns_nsroot_profile",

    "username": "admin",

    "password": "admin",

    "network_interfaces":

    [

        {

            "port_name": "10/1"

        },

        {

            "port_name": "10/2"

        }

    ]

}

}
```

リソースの詳細と統計を取得する

SDXリソースの詳細は、次の方法で取得できます。

- SDXアプライアンス上の特定のリソースの詳細を取得するには、URLでそのリソースのIDを指定します。
- 何らかのフィルターに基づいてリソースのプロパティを取得するには、URLでフィルター条件を指定します。

URLの形式は次のとおりです: `http://<IP>/nitro/v2/config/<resource_type>?filter=<property1>:<value>,<property2>:<value>`

- リクエストによってアプライアンスから多数のリソースが返される可能性がある場合、それらを「ページ」に分割し、ページごとに取得することで、これらの結果をチャンクで取得できます。

たとえば、53個のNetScalerインスタンスを持つSDX上のすべてのNetScalerインスタンスを取得したいとします。53個すべてを1つの大きな応答で取得する代わりに、結果をそれぞれ10個のNetScalerインスタンスのページに分割するように構成し（合計6ページ）、その後、サーバーからページごとに取得します。

ページサイズクエリ文字列パラメータでページ数を指定し、ページ番号クエリ文字列パラメータを使用して取得したいページ番号を指定します。URLの形式は次のとおりです: `http://<IP>/nitro/v2/config/<resource_type>?pageno=<value>&pagesize=<value>`

すべてのページを取得する必要はありませんし、ページを順番に取得する必要もありません。各リクエストは独立しており、リクエスト間でページサイズの設定を変更することもできます。

注: リクエストによって返される可能性のあるリソースの数を把握するには、リソース自体ではなく、返されるリソースの数を要求するために、countクエリ文字列パラメータを使用できます。利用可能なNetScalerインスタンスの数を取得するには、URLは次のようになります

`http://<IP>/nitro/v2/config/<resource_type>?count=yes`

ID 123456aのNetScalerインスタンスの構成情報を取得するには:

- **URL**
- **HTTPメソッド GET**

リソースを更新する

既存のSDXリソースを更新するには、PUT HTTPメソッドを使用します。HTTPリクエストペイロードで、変更する必要がある名前とその他の引数を指定します。たとえば、ID 123456aのNetScalerインスタンスの名前をvpx2に変更するには、次のようになります。

- **URL**
- **HTTPメソッド**
- **リクエストペイロード**
 - **ヘッダー**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

。ペイロード

```
{  
  
  "ns":  
  
  {  
  
    "name": "vpx2",  
  
    "id": "123456a"  
  
  }  
  
}
```

リソースを削除する

既存のリソースを削除するには、URLで削除するリソースの名前を指定します。たとえば、ID 123456aのNetScalerインスタンスを削除するには、次のようになります。

- URL
- HTTPメソッド
- リクエスト

。ヘッダー

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

一括操作

複数のリソースを同時に照会または変更できるため、ネットワークトラフィックを最小限に抑えることができます。たとえば、同じ操作で複数のNetScaler SDXアプライアンスを追加できます。また、1つのリクエストで異なるタイプのリソースを追加することもできます。

一括操作内の一部の操作の失敗に対応するため、NITROでは以下のいずれかの動作を設定できます。

- **終了。** 最初のエラーが発生した場合、実行は停止します。エラー発生前に実行されたコマンドはコミットされます。
- **続行。** 一部のコマンドが失敗しても、リスト内のすべてのコマンドが実行されます。

注: `X-NITRO-ONERROR` パラメータを使用して、リクエストヘッダーで必要な動作を設定します。

1つの操作で2つのNetScalerリソースを追加し、1つのコマンドが失敗しても続行するには:

- **URL。**
- **HTTPメソッド。**
- **リクエストペイロード。**

- **ヘッダー**

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue

Content-Type:application/vnd.com.citrix.sdx.ns+json

X-NITRO-ONERROR:continue
```

- **ペイロード**

```
{

  "ns":

  [

    {

      "name":"ns_instance1",

      "ip_address":"10.70.136.5",

      "netmask":"255.255.255.0",

      "gateway":"10.70.136.1"

    },
```

```

    {
        "name": "ns_instance2",
        "ip_address": "10.70.136.8",
        "netmask": "255.255.255.0",
        "gateway": "10.70.136.1"
    }
]
}

```

複数のリソース (NetScalerと2人のMPSユーザー) を1つの操作で追加し、1つのコマンドが失敗しても続行するには:

- URL。
- HTTPメソッド。 POST
- リクエストペイロード。
 - ヘッダー

```
Cookie:NITRO_AUTH_TOKEN=tokenvalue
```

```
Content-Type:application/vnd.com.citrix.sdx.ns+json
```

```
X-NITRO-ONERROR:continue
```

- ペイロード

```

{
    "ns":
    [
        {

```

```
        "name": "ns_instance1",

        "ip_address": "10.70.136.5",

        "netmask": "255.255.255.0",

        "gateway": "10.70.136.1"

    },

    {

        "name": "ns_instance2",

        "ip_address": "10.70.136.8",

        "netmask": "255.255.255.0",

        "gateway": "10.70.136.1"

    }

],

"mpuser":

[

    {

        "name": "admin",

        "password": "admin",

        "permission": "superuser"

    },

    {

        "name": "admin",

        "password": "admin",
```

```
        "permission": "superuser"
    }
]
}
```

例外処理

エラーコードフィールドは、操作のステータスを示します。

- エラーコードが0の場合、操作は成功したことを示します。
- ゼロ以外のエラーコードは、NITROリクエストの処理におけるエラーを示します。

エラーメッセージフィールドは、簡単な説明と障害の性質を提供します。

NITROの仕組み

NITROインフラストラクチャは、クライアントアプリケーションと、NetScaler SDXアプライアンス上で動作するNITRO Webサービスで構成されています。クライアントアプリケーションとNITRO Webサービス間の通信は、HTTPまたはHTTPSを使用するRESTアーキテクチャに基づいています。

図1. NITROワークフロー

NITROインフラ(/en-us/sdx/media/ns-nitro-infra.png)

ワークフローの詳細な手順:

1. クライアントアプリケーションは、RESTリクエストメッセージをNITRO Webサービスに送信します。SDKを使用する場合、API呼び出しは適切なRESTリクエストメッセージに変換されます。
2. WebサービスはRESTリクエストメッセージを処理します。
3. NITRO Webサービスは、対応するRESTレスポンスメッセージをクライアントアプリケーションに返します。SDKを使用する場合、RESTレスポンスメッセージはAPI呼び出しに対する適切なレスポンスに変換されます。

ネットワーク上のトラフィックを最小限に抑えるため、リソースの完全な状態をサーバーから取得します。リソースの状態をローカルで変更します。その後、1回のネットワークトランザクションでサーバーにアップロードし直します。

注: リソースに対するローカル操作（プロパティの変更）は、オブジェクトの状態が明示的にアップロードされるまで、サーバー上の状態には影響しません。

NITRO APIは本質的に同期型です。つまり、クライアントアプリケーションは、別のNITRO APIを実行する前に、NITRO Webサービスからの応答を待ちます。

ジャバ SDK

SDX NITRO APIは、そのスコープと目的に応じて、システムAPIと構成APIに分類されます。NITRO操作のトラブルシューティングも可能です。

システムAPI

NITROを使用するための最初のステップは、SDXアプライアンスとのセッションを確立し、管理者の資格情報を使用してセッションを認証することです。

アプライアンスのIPアドレスと、アプライアンスに接続するためのプロトコル（HTTPまたはHTTPS）を指定して、`nitro_service`クラスのオブジェクトを作成します。次に、このオブジェクトを使用して、管理者のユーザー名とパスワードを指定してアプライアンスにログオンします。

注: そのアプライアンスにユーザーアカウントが必要です。実行できる構成操作は、アカウントに割り当てられている管理ロールによって制限されます。

次のサンプルコードは、HTTPSプロトコルを使用してIPアドレス10.102.31.16のSDXアプライアンスに接続します。

```
//Specify the IP address of the appliance and service type

nitro_service nitroservice = new nitro_service ("10.102.31.16", "https");


//Specify the login credentials

nitroservice.login("nsroot", "verysecret");
```

注: 以降のアプライアンスでのすべてのNITRO操作で、`nitro_service` オブジェクトを使用してください。

アプライアンスから切断するには、次のように `logout()` メソッドを呼び出します。

```
nitroservice.logout();
```

構成API

NITROプロトコルは、SDXアプライアンスのリソースを構成するために使用できます。

リソースを構成するためのAPIは、`com.citrix.sdx.nitro.resource.config.<resource_type>`という形式のパッケージまたは名前空間にグループ化されています。これらの各パッケージまたは名前空間には、リソースを構成するためのAPIを提供する<resource_type>という名前のクラスが含まれています。

たとえば、NetScalerリソースには、`com.citrix.sdx.nitro.resource.config.ns`パッケージまたは名前空間があります。

リソースクラスは、他の多くの操作を実行するためのAPIを提供します。これらの操作には、リソースの作成、リソースの詳細と統計の取得、リソースの更新、リソースの削除、およびリソースに対する一括操作の実行が含まれます。

リソースの作成

SDXアプライアンスでリソース（例：NetScalerインスタンス）を作成するには、次の手順を実行します。

1. 対応するプロパティ名を使用して、リソースの必須プロパティの値を設定します。結果として、リソースに必要な詳細を含むリソースオブジェクトが作成されます。注：これらの値はクライアントにローカルで設定されます。オブジェクトがアップロードされるまで、値はアプライアンスに反映されません。
2. 静的 `add()` メソッドを使用して、リソースオブジェクトをアプライアンスにアップロードします。

次のサンプルコードは、SDXアプライアンスに「`ns_instance`」という名前のNetScalerインスタンスを作成します。

```
ns newns = new ns();

//Set the properties of the NetScaler locally
```

```
newns.set_name("ns_instance");

newns.set_ip_address("10.70.136.5");

newns.set_netmask("255.255.255.0");

newns.set_gateway("10.70.136.1");

newns.set_image_name("nsvpx-9.3.45_nc.xva");

newns.set_profile_name("ns_nsroot_profile");

newns.set_vm_memory_total(new Double(2048));

newns.set_throughput(new Double(1000));

newns.set_pps(new Double(1000000));

newns.set_license("Standard");

newns.set_username("admin");

newns.set_password("admin");


int number_of_interfaces = 2;

network_interface[] interface_array = new
network_interface[number_of_interfaces];


//Adding 10/1

interface_array[0] = new network_interface();

interface_array[0].set_port_name("10/1");


//Adding 10/2
```

```
interface_array[1] = new network_interface();

interface_array[1].set_port_name("10/2");

newns.set_network_interfaces(interface_array);

//Upload the NetScaler instance

ns result = ns.add(nitroservice, newns);
```

リソースの詳細の取得

SDXアプライアンス上のリソースのプロパティを取得するには、次の手順を実行します。

1. get() メソッドを使用して、アプライアンスから構成を取得します。結果はリソースオブジェクトです。
2. 対応するプロパティ名を使用して、オブジェクトから必要なプロパティを抽出します。

次のサンプルコードは、すべてのNetScaler®リソースの詳細を取得します。

```
//Retrieve the resource object from the SDX appliance

ns[] returned_ns = ns.get(nitroservice);

//Extract the properties of the resource from the object

System.out.println(returned_ns[i].get_ip_address());

System.out.println(returned_ns[i].get_netmask());
```

リソース統計の取得

SDXアプライアンスは、その機能の使用状況に関する統計を収集します。これらの統計はNITROを使用して取得できます。

次のサンプルコードは、ID 123456a のNetScalerインスタンスの統計を取得します。

```
ns obj = new ns();

obj.set_id("123456a");

ns stats = ns.get(nitroservice, obj);

System.out.println("CPU Usage:" + stats.get_ns_cpu_usage());

System.out.println("Memory Usage:" + stats.get_ns_memory_usage());

System.out.println("Request rate/sec:" +stats.get_http_req());
```

リソースの更新

アプライアンス上の既存のリソースのプロパティを更新するには、次の手順を実行します。

1. id プロパティを更新するリソースのIDに設定します。
2. リソースの必須プロパティの値を、対応するプロパティ名を使用して設定します。結果はリソースオブジェクトになります。注: これらの値はクライアントにローカルに設定されます。オブジェクトがアップロードされるまで、これらの値はアプライアンスに反映されません。
3. update() メソッドを使用して、リソースオブジェクトをアプライアンスにアップロードします。

次のサンプルコードは、ID 123456a の NetScaler インスタンスの名前を「ns_instance_new」に更新します。

```
ns update_obj = new ns();

//Set the ID of the NetScaler to be updated

update_obj.set_id("123456a");

//Get existing NetScaler details

update_obj = ns.get(nitroservice, update_obj);
```

```
//Update the name of the NetScaler to "ns_instance_new" locally

update_obj.set_name("ns_instance_new");


//Upload the updated NetScaler details

ns result = ns.update(nitroservice, update_obj);
```

リソースの削除

既存のリソースを削除するには、削除するリソースのIDを引数として渡し、リソースクラスの静的メソッド `delete()` を呼び出します。

次のサンプルコードは、ID 1 の NetScaler インスタンスを削除します。

```
ns obj = new ns();

obj.set_id("123456a");

ns.delete(nitroservice, obj);
```

一括操作

複数のリソースを同時に照会または変更できるため、ネットワークトラフィックを最小限に抑えることができます。たとえば、同じ操作で複数の NetScaler SDX アプライアンスを追加できます。

各リソースクラスには、リソースの追加、更新、削除のためにリソースの配列を受け取るメソッドがあります。一括操作を実行するには、各操作の詳細をローカルで指定し、その詳細を一度にサーバーに送信します。

一括操作内の一部の操作の失敗を考慮するために、NITRO では次のいずれかの動作を構成できます。

- **終了。** 最初のエラーが発生すると、実行は停止します。エラーの前に実行されたコマンドはコミットされます。
- **続行。** 一部のコマンドが失敗しても、リスト内のすべてのコマンドが実行されます。

注: アプライアンスとの接続を確立する際に、必要な動作を構成するには、`onerror` パラメータを `nitro_service()` メソッドで設定します。

次のサンプルコードは、1回の操作で2つのADCアプライアンスを追加します。

```
ns[] newns = new ns[2];

//Specify details of first NetScaler

newns[0] = new ns();

newns[0].set_name("ns_instance1");

newns[0].set_ip_address("10.70.136.5");

newns[0].set_netmask("255.255.255.0");

newns[0].set_gateway("10.70.136.1");

...

...

...

//Specify details of second NetScaler

newns[1] = new ns();

newns[1].set_name("ns_instance2");

newns[1].set_ip_address("10.70.136.8");

newns[1].set_netmask("255.255.255.0");

newns[1].set_gateway("10.70.136.1");

...
```

```
...
```

```
//upload the details of the NetScalers to the NITRO server
```

```
ns[] result = ns.add(nitroservice, newns);
```

例外処理

エラーコードフィールドは、操作のステータスを示します。

- エラーコードが0の場合、操作が成功したことを示します。
- ゼロ以外のエラーコードは、NITROリクエストの処理におけるエラーを示します。

エラーメッセージフィールドは、簡潔な説明と障害の性質を提供します。

`com.citrix.sdx.nitro.exception.nitro_exception`クラスは、NITRO APIの実行におけるすべての例外をキャッチします。例外に関する情報を取得するには、`getErrorCode()` メソッドを使用できます。

エラーコードの詳細については、`<NITRO_SDK_HOME>/doc` フォルダーで利用可能なAPIリファレンスを参照してください。

fix

This is the content for the sample heading topic. It is hidden from the main table of contents but remains accessible via links.